Krishna's Question Bank

Algebra

(*For B.A. and B.Sc. I year students of All Colleges affiliated to Allahabad State University*)

As per Allahabad State University Syllabus

(*w.e.f.* 2017-2018)

By

A. R. Vasishtha
Retired Head, Dep't. of Mathematics
Meerut College, Meerut (U.P.)

Hemlata Vasishtha
M.Sc. (Gold Medalist), Ph.D.
C.C.S. University, Meerut (U.P.)

KRISHNA Prakashan Media (P) Ltd.
KRISHNA HOUSE, 11, Shivaji Road, Meerut-250 001 (U.P.), India

Jai Shri Radhey Shyam

Dedicated
to
Lord
Krishna

Authors & Publishers

Brief Contents

Krishna's

ALGEBRA

Chapters

Chapters

Chapter-1

Properties of Integers

Comprehensive Problems 1

Problem 1: *If x, y, z are any integers, then prove that*

(i) $x(y-z) = xy - xz$ *(ii)* $(x+z)-(y+z) = x-y$.

Solution : Let $x = [a, b]$, $y = [c, d]$, $z = [e, f]$.

Then we have $-x = [b, a]$, $-y = [d, c]$, $-z = [f, e]$.

(i) $x(y-z) = x\{y+(-z)\}$

$= xy + x(-z)$ [$\because$ Multiplication distributes addition in **I**]

$= xy + [a, b][f, e] = xy + [af + be, ae + bf]$

$= xy + (-[ae + bf, af + be]) = xy - ([ae + bf, af + be])$

$= xy - ([a, b][e, f]) = xy - xz.$

(ii) $(x+z)-(y+z) = ([a, b]+[e, f])-([c, d]+[e, f])$

$= [a+e, b+f]-[c+e, d+f]$

$= [a+e, b+f]+[d+f, c+e]$

$= [a+e+d+f, b+f+c+e]$

$= [a+d+e+f, b+c+e+f]$

$= [a+d, b+c]$, since $(a+d+e+f, b+c+e+f) \sim (a+d, b+c)$

$= [a, b]+[d, c] = [a, b]+(-[c, d]) = [a, b]-[c, d] = x-y.$

Problem 2: *Prove that the relation of divisibility in the set of integers is reflexive, transitive but not symmetric.*

Solution: The relation is reflexive. For every $a \in \mathbf{I}$, we have $a = a1$ where $1 \in \mathbf{I}$. Therefore $a \mid a$ for all $a \in \mathbf{I}$. Hence the relation is reflexive.

The relation is not symmetric. We have $2 \mid 8$ but 8 is not a divisor of 2. Therefore this relation is not symmetric.

The relation is transitive. *For every $a, b, c \in \mathbf{I}$, we have $a \mid b$ and $b \mid c \Rightarrow a \mid c$.*

We have $a \mid b \Rightarrow b = ax$ for some $x \in \mathbf{I}$.

Also $b \mid c \Rightarrow c = by$ for some $y \in \mathbf{I}$.

From these we get

$c = by$

$= (ax)y$ [$\because b = ax$]

$= a(xy)$ where $xy \in \mathbf{I}$.

$\therefore$ $a \mid c$.

Problem 3: *Prove that the number of positive primes is infinite.*

Solution: Suppose there are only a finite number of positive primes, say n, and they are $p_1, p_2, p_3, \ldots, p_n$ arranged in order of magnitude.

Now form the product $a = p_1 \cdot p_2 \cdot p_3 \ldots p_n$ and consider the integer $a + 1$. As no one of the p's is a divisor of $a + 1$, we conclude that either $a + 1$ is a prime $> p_n$ or has a prime $> p_n$, as factor. But this contradicts our assumption that p_n is the greatest prime.

Hence the number of positive primes is infinite.

Problem 4: *Find* $(427, 616)$ *and express it in the form*

$$427m + 616n.$$

Solution: By repeated application of division algorithm, we get

$$616 = (427).1 + 189, \quad \ldots(1)$$
$$427 = (189).2 + 49, \quad \ldots(2)$$
$$189 = (49).3 + 42, \quad \ldots(3)$$
$$49 = (42).1 + 7, \quad \ldots(4)$$
$$42 = (7).6 + 0. \quad \ldots(5)$$

Hence $(427, 616) = 7$.

Now from the last but one equation, *i.e.*, from (4), we get

$$7 = 49 - (42).1$$
$$= 49 - [189 - (49).3].1 \quad \text{[By (3)]}$$
$$= (49).4 - 189$$
$$= [427 - (189).2].4 - 189 \quad \text{[By (2)]}$$
$$= (427).4 - (189).9$$
$$= (427).4 - [616 - (427).1].9 \quad \text{[By (1)]}$$
$$= (427).13 + (616)(-9).$$

Problem 5: *If* $(a, b) = 1$, $a \mid c, b \mid c$, *then prove that* $ab \mid c$.

Solution: Put $d = 1$ in example 9 and give the complete solution of example 9.

Problem 6: *Find the least positive incongruent solutions of :*

(i) $259x \equiv 5$ *(mod 11)* *(ii)* $11x \equiv 2$ *(mod 317).*

Solution: (i) We have $(259, 11) = 1$. Therefore the congruence

$$259x \equiv 5 \pmod{11} \quad \ldots(1)$$

has a single incongruent solution.

We have $259 = 23.11 + 6$ where $0 \le 6 < 11$

or $259 = 253 + 6$.

Now $253x \equiv 0 \pmod{11}$. $\ldots(2)$

From (1) and (2), we get

$$259x - 253x \equiv 5 - 0 \pmod{11}$$

or $6x \equiv 5 \pmod{11}$. $\ldots(3)$

Now $5 \equiv 60 \bmod (11)$. $\ldots(4)$

[Note that 60 is the least positive integer divisible by 6 and also congruent to 5 modulo 11.]

From (3) and (4), we get

$$6x \equiv 60 \pmod{11} \quad \text{or} \quad 6x \equiv 6.10 \pmod{11}$$

or $x \equiv 10 \pmod{11}$ $[\because (6, 11) = 1]$

showing that $x = 10$ is a solution.

Obviously 10 is the least positive integer in the residue class $[10] \in \mathbf{I}_{11}$. Hence $x = 10$ is the required solution.

(ii) We have $(11, 317) = 1$. Therefore the congruence $11x \equiv 2 \pmod{317}$ has a single incongruent solution. Here the modulus 317 is large. So we proceed as follows :
Since $(11, 317) = 1$, therefore we can find integers m and n such that

$$1 = 11m + 317n$$

We have
$317 = 11.28 + 9$
$11 = 9.1 + 2$
$9 = 2.4 + 1$
$2 = 1.2.$

Now
$1 = 9 - 2.4 = 9 - (11 - 9.1).4 = 5.9 - 4.11$
$= 5.(317 - 11.28) - 4.11 = 5.317 + (-144).11$

$\therefore$ $2 = 10.317 + (-288).11$

Now $11x \equiv 2 \pmod{317}$ is equivalent to
$11x \equiv 10.317 + (-288)\,11 \pmod{317}$
or $11x \equiv (-288)\,11 \pmod{317}$

showing that $x = -288$ is a solution of the given congruence.
Now $-288 = -317 + 29$. Therefore 29 is the least positive integer in the residue class $[-288] \in \mathbf{I}_{317}$. Hence $x = 29$ is the required solution.

Problem 7: *Find the least positive incongruent solutions of*

(i) $2x + 1 \equiv 4$ *(mod 5)* *(ii)* $2x + 1 \equiv 4$ *(mod 10)*

(iii) $51x \equiv 32$ *(mod 7)* *(iv)* $7x \equiv 5$ *(mod 256)*

(v) $104x \equiv 16$ *(mod 296)* *(vi)* $45x \equiv 24$ *(mod 348).*

Solution: Proceed as in Problem 6.

Ans. (i) 4 (ii) no solution (iii) 2 (iv) 147 (v) 3 (vi) 16.

Hints to Objective Type Questions

Multiple Choice Questions

1. See Example 1.
2. See Problem 2 of Comprehensive Problems 1.
3. See article 14.
4. See Example 7.

Fill in the Blank(s)

1. See article 15 (Theorem 2).
2. See Problem 4 of Comprehensive Problems 1.
3. See Example 10.

True or False

1. See Theorem 8 of article 18.
2. See Theorem 1 of article 19.
3. See Theorem 1 of article 16.
4. See article 13. Definition of associates.

○○○

Chapter-2

Equivalence Relations and Partitions

Comprehensive Problems 1

Problem 1: *Prove that the relation "congruence modulo m" is an equivalence relation in the set of integers.* **(Avadh 2006, 10; Rohilkhand 06; Agra 06; Kumaun 12)**

Solution: Let **I** be the set of integers. If m is any given positive integer and $a, b \in \mathbf{I}$, then we say that $a \equiv b \pmod m$ if $m \mid (a - b)$ *i.e.*, if m is a divisor of $a - b$. We shall prove that this defines an equivalence relation in the set **I**.

Reflexivity: Let a be any integer. Then $a - a = 0$ and $m \mid 0$ because we can write $0 = m.0$. Thus $a \equiv a \pmod m \ \forall\, a \in \mathbf{I}$. Therefore the relation is reflexive.

Symmetry: Let $a, b \in \mathbf{I}$ be such that $a \equiv b \pmod m$. Then

$$a \equiv b \pmod m \Rightarrow m \mid (a - b)$$

$\Rightarrow$ $a - b = km$, where k is some integer

$\Rightarrow$ $b - a = (-k)\, m$, where $-k$ is also an integer

$\Rightarrow$ $m \mid (b - a) \quad \Rightarrow \quad b \equiv a \pmod m$.

Thus $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$. Therefore the relation is symmetric.

Transitivity: Let $a, b, c \in \mathbf{I}$ be such that

$$a \equiv b \pmod m,\ b \equiv c \pmod m.$$

Then we have and $m \mid (b - c)$

$\Rightarrow$ $a - b = k_1 m$ and $b - c = k_2 m$, where k_1, k_2 are some integers

$\Rightarrow$ $(a - b) + (b - c) = k_1 m + k_2 m$

$\Rightarrow$ $m \mid (a - c) \Rightarrow a \equiv c \pmod m$.

Thus $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$. Therefore the relation is transitive.

Since the relation of "congruence modulo m" on the set of integers is reflexive, symmetric and transitive, therefore it is an equivalence relation.

Problem 2: *Define an equivalence relation . If R is a relation in the natural numbers* **N** *defined by the open sentence "x – y is divisible by 7", that is* $R = \{(x, y) : x \in \mathbf{N},\ y \in \mathbf{N}, (x - y)$ *is divisible by 7}, prove that R is an equivalence relation.*

Solution: Refer article 19 and proceed as in Illustration 2.

Problem 3: *Let* **I** *be the set of all integers. Let a relation a R b,* $(a, b \in \mathbf{I})$ *be defined if* $a - b$ *is an even integer. Show that R is an equivalence relation and describe the equivalence classes.*

Solution: Proceed as in problem 1.

Problem 4: *Define an equivalence relation and check if in the set of natural numbers the relation 'x is a multiple of y' is an equivalence relation.*

Solution: See article 19.

Let N in the set of Natural numbers.

Let $a \in N$

We have every natural number is the factor of itself

$\therefore$ $aRa \Rightarrow$ relation R in reflexive

Let $a,b \in N$

If b is the factor of a then a is not a factor of b

i.e., $aRb \Rightarrow b \notin a$

so relation R is not symmetric.

Let $a,b,c, \in N$

If b is the factor of a and c is the factor of b

Then aRb and $bRc \Rightarrow aRc$

$\therefore$ Relation R is transitive.

Problem 5: *Define a relation. Give an example of a relation which is*

(i) symmetric and reflexive but not transitive.

(ii) symmetric and transitive but not reflexive.

(iii) reflexive but neither symmetric nor transitive.

Solution: Consider the set $S = \{1, 2, 3\}$. Then

(i) $R_1 = \{(1,1), (2,2), (3,3), (2,3), (3,2), (1,2), (2,1)\}$ is a relation on S such that R_1 is reflexive and symmetric but not transitive.

Observe that $(1, 2) \in R_1$, $(2, 3) \in R_1$ but $(1, 3) \notin R_1$ and so R_1 is not transitive.

(ii) $R_2 = \{(1,1), (2,2), (1,2), (2,1)\}$ is a relation on S such that R_2 is symmetric and transitive but not reflexive. Observe that $(3, 3) \notin R_2$ and so R_2 is not reflexive.

(iii) $R_3 = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$ is a relation on S such that R_3 is reflexive but is neither symmetric nor transitive.

Problem 6: *If R and S are two equivalence relations, then check $R \cup S$ for*

(i) reflexivity, (ii) transitivity and (iii) symmetry.

Solution: Let R and S are two equivalence in X relation.

Therefore, $R \subseteq X \times X$ and $S \subseteq X \times X$

$\therefore$ $R \cup S \subseteq X \times X$

(i) $(a,a) \in R \ \forall \ a \in X$

$(a,a) \in R \ \forall \ a \in X$

$\therefore$ $(a,a) \in R \cup S$

$\therefore$ $R \cup S$ is reflexive.

(ii) $(a,b) \in R \cup S$

$\Rightarrow$ $(a,b) \in R$ or $(a,b) \in S$

$\Rightarrow$ $(b,a) \in R$ or $(b,a) \in S$

$\Rightarrow$ $(b,a) \in R \cup S$

$\therefore$ $R \cup S$ is symmetric.

(iii) Let $(a,b) \in R \cup S, (b,c) \in R \cup S$

$\Rightarrow$ $[(a,b) \in R$ or $(a,b) \in S], [(b,c) \in R$ or $(b,c) \in S]$

$\Rightarrow$ $[(a,b) \in R], [(b,c) \in R$ or $(b,c) \in S]$ or $[(a,b) \in S], [(b,c) \in R$ or $(b,c) \in S]$

$\Rightarrow$ (a,c) not necessarily $\in R$ or (a,c) not necessarily $\in S$

$\Rightarrow$ (a,c) not necessarily $\in R \cup S$

$\therefore$ $R \cup S$ is not necessarily transitive.

Problem 7: *Let a relation R be defined by* $R = (4,5), (1,4), (4,6), (7,6), (3,7)$. *Find*

(i) $R \circ R$, *(ii)* $R^{-1} \circ R$.

Solution: Let a relation R be defined by

$R = \{(4,5), (1,4), (4,6), (7,6), (3,7)\}$

then $R^{-1} = \{(5,4), (4,1), (6,4), (6,7), (7,3)\}$

(i) We observe that

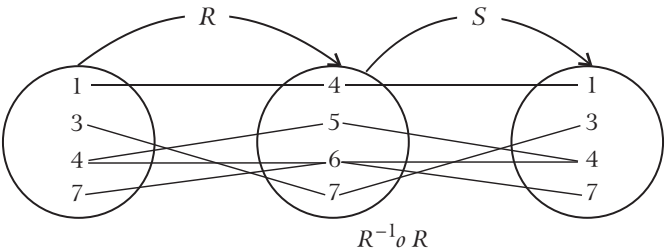
$(4,5) \in R$ and $(1,4) \in R \Rightarrow (1,5) \in R \circ R$,

$(4,6) \in R$ and $(1,4) \in R \Rightarrow (1,6) \in R \circ R$

and $(7,6) \in$ and $(3,7) \in R$ $(3,6) \in R \circ R$

$\therefore$ $R \circ R = \{(1,5)\ (1,6)\ (3,6)\}$

(ii)



$R^{-1} \circ R$

$1 \xrightarrow{R} 4 \xrightarrow{R^{-1}} 1 \Rightarrow (1,1) \in R^{-1} \circ R$

$3 \xrightarrow{R} 7 \xrightarrow{R^{-1}} 3 \Rightarrow (3,3) \in R^{-1} \circ R$

$4 \xrightarrow{R} 5 \xrightarrow{R^{-1}} 4 \Rightarrow (4,4) \in R^{-1} \circ R$

$4 \xrightarrow{R} 6 \xrightarrow{R^{-1}} 7 \Rightarrow (4,7) \in R^{-1} \circ R$

$7 \xrightarrow{R} 6 \xrightarrow{R^{-1}} 4 \Rightarrow (7,4) \in R^{-1} \circ R$

$7 \xrightarrow{R} 6 \xrightarrow{R^{-1}} 7 \Rightarrow (7,7) \in R^{-1} \circ R$

$\therefore$ $R^{-1} \circ R = \{(1,1), (3,3), (4,4), (4,7), (7,4), (7,7)\}$.

Problem 8: *If R, S, T be relations on a set X, then prove that*

(i) $(R^{-1})^{-1} = R$, *(ii)* $R \circ (S \circ T) = (R \circ S) \circ T$

(iii) $R \circ I_X = I_X \circ R = R$.

Solution: $(R^{-1})^{-1} = R$ can be proved by using the definition of inverse relation twice. Proceed as in Theorem 2 and Theorem 4 of article 8.

Problem 9: *Which of the following statements is true / false ? Give reasons to support your answer.*

(i) A relation R is an equivalence relation if it is reflexive and symmetric.

(ii) Union of two reflexive relations is a reflexive relation.

Solution: (i) False.

Because an equivalence relation is reflexive, symmetric and transitive.

(ii) True.

Let $R = \{(1, 1)(1, 2)(2, 1),(2, 2)\}$ is reflexive

and $S = \{(3, 3), (3, 4), (4, 3), (4, 4)\}$ is reflexive

$\therefore$ $R \cup S$ is also reflexive.

Problem 10: *Which of the following relations in the set of real numbers are equivalence relations ?*

(i) $a\ R\ b$ *iff* $|a| \leq b$. *(ii)* $a\ R\ b$ *iff* $|a| > |b|$. *(iii)* $a\ R\ b$ *iff* $|a| \neq |b|$.

Solution: Let E denote the set of real numbers.

(i) The given relation R on the set E is not reflexive.

For example $-6 \in E$. We have $|-6| = 6$ and the statement $6 \leq -6$ is not true. Thus -6 is not R-related to -6 because the statement $|-6| \leq -6$ is not true.

Thus there exist elements in E which are not R-related to themselves. Therefore the relation R is not reflexive. Hence it is not an equivalence relation.

(ii) The given relation R on the set E is not reflexive. For example $3 \in E$. We have $|3| = 3$. The statement $|3| > |3|$ is false. Thus 3 is not R-related to 3 because the statement $|3| > |3|$ is not true.

Thus there exist elements in E which are not R-related to themselves. Therefore the relation R on the set E is not reflexive. Hence it is not an equivalence relation.

(iii) The given relation R on the set E is not reflexive. For example $4 \in E$. The statement $|4| \neq |4|$ is false and so 4 is not R-related to itself. Since the relation R on the set E is not reflexive, therefore it cannot be an equivalence relation.

Problem 11: *A relation* $R = \{(1, 1), (1, 2), (2, 1)\}$ *is defined on the set* $A = \{1, 2, 3\}$. *Check if R is reflexive, symmetric and transitive.*

Solution: $R = \{(1, 1)(1, 2), (2, 1)\}$ in defined on set $\{1, 2, 3\}$.

(i) Here $2\,R\,2$ so it is not reflexive.

(ii) Here $1\,R\,2 \Leftrightarrow 2\,R\,1$ so it is symmetric.

(iii) Here $1\,R\,2$ but no any relation to third element of set S so it is not transitive.

Problem 12: *Let S be the set of all points in a plane. Let R be a relation such that for any two points a and b , a R b if b is within one inch from a. Show that R is reflexive and symmetric but, not transitive.*

Solution: **(i) *R* is reflexive:** Let a be any arbitrary point $\in S$. The distance of a from a is zero and therefore a is within one inch from a. Hence $\forall\ a \in S$, we have $a\ R\ a$. Thus R is reflexive.

(ii) *R* is symmetric: Suppose we have $a\ R\ b$ *i.e.*, b is within one inch from a. Now the distance of a from b is equal to the distance of b from a. Therefore if b is within one inch from a, then a is also within one inch from b. So $a\ R\ b$ implies $b\ R\ a$, Therefore R is symmetric.

(iii) *R* is not transitive: Suppose, we have $a\ R\ b$ and $b\ R\ c$. Then b is within one inch from a and c is within one inch from b. Suppose a, b and c are in the same straight line and b lies between a and c. Let the distance of b from a be $3/4$ inch and the distance of c from b also $3/4$ inch. Then the distance of c from a is $3/4 + 3/4$ *i.e.*, $1\frac{1}{2}$ inches. Thus c is not within one inch from a and therefore a is not R-related to c. Hence R is not transitive.

Problem 13: *Show that the relation R in the set of natural numbers* **N** *defined by a R b if a divides b, is reflexive and transitive but not symmetric.* **(Kumaun 2007)**

Solution: **(i) *R* is reflexive:** For every $a \in \mathbf{N}$, a is a divisor of a *i.e.*, $a\ R\ a$. Hence R is reflexive.

(ii) *R* is transitive: Suppose $a\ R\ b$ and $b\ R\ c$. Then a is a divisor of b and b is a divisor of c. If a is a divisor of b and b is a divisor of c, then a is a divisor of c *i.e.*, $a\ R\ c$. Thus $a\ R\ b$ and $b\ R\ c \Rightarrow a\ R\ c$. Therefore R is transitive.

(iii) *R* is not symmetric: We have $4 \in \mathbf{N}$, $2 \in \mathbf{N}$, 2 is a divisor of 4 *i.e.*, $2\ R\ 4$, but 4 is not a divisor of 2 *i.e.*, 4 is not R-related to 2. Thus $(2, 4) \in R \Rightarrow (4, 2) \notin R$. Hence R is not symmetric.

Problem 14: *Show that the relation "greater than" denoted by* $>$ *in the set of natural numbers* **N** *is transitive but is neither reflexive nor symmetric.*

Solution: **(i) *R* is not reflexive:** We have $3 \in \mathbf{N}$, but 3 is not greater than 3 *i.e.*, 3 is not R-related to 3. Therefore R is not reflexive.

(ii) *R* is not symmetric: We have $4 \in \mathbf{N}$, $2 \in \mathbf{N}$, 4 is greater than 2 *i.e.*, $4\ R\ 2$ but 2 is not greater than 4 *i.e.*, $(2, 4) \notin R$. Therefore R is not symmetric.

(iii) *R* is transitive: Suppose $a\ R\ b$ and $b\ R\ c$. Then $a > b$ and $b > c$. Now $a > b$ and $b > c \Rightarrow a > c$ *i.e.*, $a\ R\ c$. Therefore R is transitive.

Problem 15: *Prove that the relation R in the set of integers* **I** *defined by a R b if a and b are both odd is symmetric and transitive but not reflexive.*

Solution: **(i) *R* is not reflexive:** We have $2 \in \mathbf{I}$. But 2 is not R-related to 2, since 2 and 2 are not both odd. Therefore R is not reflexive.

(ii) *R* is symmetric: Suppose we have $a\ R\ b$. Then a and b are both odd. Now if a and b are both odd then b and a are both odd *i.e.*, $b\ R\ a$. Thus $a\ R\ b \Rightarrow b\ R\ a$ and therefore R is symmetric.

(iii) *R* is transitive: Suppose we have $a\ R\ b$ and $b\ R\ c$. Then a and b are both odd as well as b and c are both odd. It implies that a and c are both odd *i.e.*, $a\ R\ c$. Thus $a\ R\ b$ and $b\ R\ c \Rightarrow a\ R\ c$. Therefore R is transitive.

Problem 16: *Prove that the relation of similarity in the set of all triangles in a plane is an equivalence relation.* **(Meerut 2013B)**

Solution: Let A be the set of all triangles in a plane. Let R be the relation in A defined as $x\ R\ y$ if and only if the triangle x is similar to the triangle y, $x \in A$, $y \in A$.

(i) **R is reflexive:** Let $x \in A$. Since every triangle is similar to itself, therefore by our definition of R, we have $x\ R\ x$.

Thus $x\ R\ x\ \forall\ x \in A$. Therefore R is reflexive.

(ii) **R is symmetric:** Let $x, y \in A$ be such that $x\ R\ y$. We have

$x\ R\ y \Rightarrow$ triangle x is similar to triangle y [By def. of R]

$\Rightarrow$ triangle y is similar to triangle x

$\Rightarrow$ $y\ R\ x$ [by def. of R].

Thus $x\ R\ y \Rightarrow y\ R\ x$. Therefore R is symmetric.

(iii) **R is transitive:** Let $x, y, z \in A$ be such that $x\ R\ y$ and $y\ R\ z$. We have

$x\ R\ y$ and $y\ R\ z$

$\Rightarrow$ triangle x is similar to triangle y and triangle y is similar to triangle z

$\Rightarrow$ triangle x is similar to triangle z

$\Rightarrow$ $x\ R\ z$ [by def. of R].

Thus $x\ R\ y$ and $y\ R\ z \Rightarrow x\ R\ z$. Therefore R is transitive.

Since R is reflexive, symmetric and transitive therefore R is an equivalence relation.

Problem 17: *Let the relation R in the set of real numbers be defined as a R b if and only if* $1 + ab > 0$. *Show that this relation is reflexive and symmetric but not transitive.*

Solution: Let S denote the set of all real numbers. Let R be a relation in S defined as $a\ R\ b$ iff $1 + ab > 0$.

(i) R is reflexive: Let a be any real number.

Then $1 + aa = 1 + a^2 > 0$, since $a^2 \geq 0$.

Thus $a\ R\ a\ \forall\ a \in S$. Therefore R is reflexive.

(ii) R is symmetric: Let a, b be any two real numbers. Then

$a\ R\ b \Rightarrow 1 + ab > 0 \Rightarrow 1 + ba > 0$ $[\because ab = ba]$

$\Rightarrow$ $b\ R\ a$.

$\therefore$ R is symmetric.

(iii) R is not transitive: Consider three real numbers $1, -\frac{1}{2}, -4$. We have

$$1 + 1\left(-\frac{1}{2}\right) = \frac{1}{2} > 0.$$

$\therefore$ $1\ R\ -\frac{1}{2}$.

Further $1 + \left(-\frac{1}{2}\right)(-4) = 3 > 0.$

$\therefore \quad -\frac{1}{2} R - 4.$

But $1 + 1(-4) = -3$ which is not greater than 0. Therefore 1 is not R-related to -4.

Thus $1\ R -\frac{1}{2}, -\frac{1}{2} R - 4$ and 1 is not R-related to -4.

$\therefore$ R is not transitive.

Problem 18: *In the set of all ordered pairs (a, b), where a, b are integers (positive, zero or negative) but $b \neq 0$, define a relation R by $(a, b)\ R\ (c, d)$ if and only if $ad = bc$.*

Show that R is an equivalence relation.

Solution: R is the pair of (a, b) and (c, d)

when $ad = bc$

(i) $(a, b)\ R\ (a, b) \Rightarrow ab = ba \ \forall\ a, b \in I$

Then it is true.

So $(a, b)\ R\ (a, b)$ is a reflexive relation.

(ii) $(a, b) R\ (c, d) \Rightarrow ad = bc \Rightarrow bc = ad$

$\Rightarrow cb = da \Rightarrow (c, d)\ R\ (a, b).$

So given relation is symmetric.

(iii) $(a, b)\ R\ (c, d)$ and $(c, d)\ R\ (e, f) \ \forall\ a, b, c, d, e, f \in I$

$\Rightarrow ad = bc$ and $cf = de \Rightarrow (ad)(cf) = (bc)(de)$

$\Rightarrow af = be \Rightarrow (a, b)\ R\ (e\ f),$

So given relation is transitive.

$\therefore$ The given relation is an equivalence relation.

Problem 19: *If R is a relation defined on real numbers x and y such that $x\ R\ y$ iff $x - y + \sqrt{2}$ is an irrational number, examine whether R is an equivalence relation or not.*

Solution: Let E denote the set of all real numbers.

(i) ***R* is reflexive:** Let $x \in E$. Then

$x - x + \sqrt{2} = \sqrt{2}$ which is an irrational number.

$\therefore$ By definition of the relation R, $x\ R\ x, \ \forall\ x \in E$.

Hence R is reflexive.

(ii) ***R* is not symmetric:** Let us take

$x = \sqrt{2}, y = 0.$

Then $\sqrt{2} - 0 + \sqrt{2} = 2\sqrt{2}$

which is an irrational number and so by definition of the relation $R, x\ R\ y$ *i.e.*, $\sqrt{2}\ R\ 0$.

But y is not R-related to x because

$y - x + \sqrt{2} = 0 - \sqrt{2} + \sqrt{2} = 0$

which is not an irrational number.

Thus there exist $x, y \in E$ such that $x\ R\ y$ but y is not R-related to x. Hence R is not symmetric.

(iii) ***R* is not transitive:** Let us take

$x = 0,\ y = \sqrt{3}, z = \sqrt{2}.$

Then $0 - \sqrt{3} + \sqrt{2}$ is an irrational number $\Rightarrow\ x\ R\ y$

and $\sqrt{3} - \sqrt{2} + \sqrt{2} = \sqrt{3}$ is an irrational number $\Rightarrow\ y\ R\ z.$

But $0 - \sqrt{2} + \sqrt{2} = 0$ is not an irrational number

$\Rightarrow$ x is not R-related to z.

Thus there exist $x, y, z \in E$ such that $x\ R\ y$ and $y\ R\ z$ but x is not R-related to z. Hence R is not transitive.

Thus R is neither symmetric nor transitive. Hence R is not an equivalence relation on the set of all real numbers.

Hints to Objective Type Questions

Multiple Choice Questions

1. Let m and n be any two different elements in **Q**. Then

$m \neq n \Rightarrow 2m \neq 2n \Rightarrow 2m + 3 \neq 2n + 3 \Rightarrow f(m) \neq f(n).$

Thus different elements in **Q** have different f – images in **Q**. Hence f is one-one.

Let y be any arbitrary element in **Q**. If $y = f(x) = 2x + 3$, we have

$x = \left(\frac{y-3}{2}\right)$ which is also a rational number.

Thus $f\left(\frac{y-3}{2}\right) = y$ *i.e.*, any arbitrary element y in **Q** is the f-images of the element $\left(\frac{y-3}{2}\right) \in \mathbf{Q}$. Hence f is onto.

2. See problem 5(i) of Comprehensive Problems 1.

3. See article 19, Illustration 2.

4. See Example 6.

5. See Example 13.

6. See problem 6 of Comprehensive Problems 1.

7. See problem 13 of Comprehensive Problems 1.

8. See problem 14 of Comprehensive Problems 1.

9. See problem 17 of Comprehensive Problems 1.

10. See problem 19 of Comprehensive Problems 1.

11. See article 11.

Fill in the Blank(s)

1. See article 2.

2. See article 2.

3. See article 2.

4. See article 1.
5. See article 1.
6. See article 8, Theorem 3.
7. See article 11.
8. See article 18.
9. See article 18.
10. See article 19.

True or False

1. Let **C** be the set of complex numbers and **R** be the set of real numbers. The mapping $f : \mathbf{C} \to \mathbf{R}$ defined by $f(z) = |z|$, $\forall\, z \in \mathbf{C}$ is neither one-one nor onto.
2. See article 2.
3. $f^{-1}\left(\frac{1}{x}\right) = x \;\forall\; x \in \mathbf{R}_0$ will not exist for $x = 0$, because $1/0$ is not a real number.
4. The mapping $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = \sin x$, $\forall\; x \in \mathbf{R}$ is one-one and onto.
5. We know that if $x \in \mathbf{R}$, then $-1 \le \cos x \le 1$. Therefore if $y \in$ the co-domain of **R** of $y > 1$ or $y < -1$, then there exists no $x \in$ the domain **R** of f such that $f(x) = \cos x = y$. Therefore the mapping is into and not onto.
6. See problem 6 of Comprehensive Problems 1.
7. See article 19.
8. See problem 5(iii) of Comprehensive Problems 1.

○○○

Chapter-3

Groups

Comprehensive Problems 1

Problem 1: *State the axioms which a set must obey so that it may form a group.*

Solution: ***Definition:*** *Let G be a non-empty set equipped with a binary operation denoted by* $\bullet$ *i.e.,* $a \bullet b$ *or more conveniently ab represents the element of G obtained by applying the said binary operation between the elements a and b of G taken in that order. Then this algebraic structure* $(G, \bullet)$ *is a group if the binary operation* $\bullet$ *satisfies the following postulates* :

1. Closure property *i.e.,* $ab \in G \ \forall \ a, b \in G.$

2. Associativity *i.e.,* $(ab)\, c = a\,(bc) \ \forall\, a, b, c \in G.$

3. Existence of identity: *There exists an element* $e \in G$ *such that* $ea = a = ae \ \forall \ a \in G$. *The element e is called the identity.*

4. Existence of Inverse: *Each element of G possesses inverse. In other words* $a \in G \Rightarrow$ *there exists an element* $b \in G$ *such that* $ba = e = ab$. *The element b is then called the* ***inverse*** *of a and we write* $b = a^{-1}$. *Thus* a^{-1} *is an element of G such that* $a^{-1}\, a = e = aa^{-1}$.

Abelian group or Commutative group: Definition:

A group G is said to be abelian or commutative if in addition to the above four postulates the following postulate is also satisfied.

5. Commutativity *i.e.,* $ab = ba \ \forall \ a, b, \in G.$

Problem 2: *Show that the following are groups:*

(i) The set **C** *of all complex numbers with respect to the operation of addition of complex numbers.*

(ii) The set **Q** *of all rational numbers with respect to addition.*

(iii) The set **R** *of all real numbers with respect to addition.*

(iv) The set $\mathbf{R_0}$ *of all non-zero real numbers with respect to multiplication.*

Solution: (i) Proceed as in Example 1 and write the complete proof yourself. Here if $x_1 + iy_1$ and $x_2 + iy_2$ are any two complex numbers, then $(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i\,(y_1 + y_2)$ is also a complex number. Thus **C** is closed for addition of complex numbers or in other words addition is a binary operation on the set of complex numbers. The addition of complex numbers is an associative operation. The zero complex number, *i.e.*, the complex number $0 + i\,0$ is identity for addition of complex numbers. Finally if $x + iy$ is any complex number, then the complex number $-x - iy$ is its additive inverse. Thus **C** is a group for addition of complex numbers.

(ii) We have $\mathbf{Q} = \left\{ \frac{a}{b} : a, b \in \mathbf{I} \text{ and } b \neq 0 \right\}$.

Write the complete proof yourself on the basis of example 1. Here the rational number 0 is the additive identity and if $x = a/b$ is any rational number, then the rational number $-a/b$ is its additive inverse.

(iii) Write the complete proof yourself on the basis of example 1. Here the real number 0 is the additive identity and if a is any real number, then the real number $-a$ is its additive inverse.

(iv) Proceed as in Example 2.

Problem 3: *(i) Define the order of a group. Show that the set of all even integers with zero is an abelian group with respect to addition.*

(ii) Show that the set $G = \{ \ldots, -4m, -3m, -2m, -m, 0, m, 2m, 3m, 4m, \ldots \}$ *of multiples of integers by a fixed integer m is a group with respect to addition.*

(iii) Show that the set **N** *of all natural numbers 1, 2, 3, 4, 5,... does not form a group with addition or multiplication but it forms a semi-group with respect to addition as well as multiplication.*

Solution: (i) See article 4. Proceed as in example 1.

(ii) **Closure Property:** Let a, b be any two elements of G. Then $a = rm$ and $b = sm$ where r and s are some integers.

Now $a + b = rm + sm = (r + s)\, m$. Since $r + s$ is also an integer, therefore $(r + s)\, m$ *i.e.*, $a + b \in G$. Thus $a + b \in G \ \forall\ a, b \in G$. Therefore G is closed with respect to addition.

Associativity: The elements of G are all integers and we know that the addition of integers is an associative composition.

Existence of Identity: $0 \in G$ and we have $0 + a = a = a + 0 \ \forall\ a \in G$. Therefore 0 is the identity.

Existence of Inverse: Let $r\, m$ be an arbitrary element of G where r is some integer.

Then $(-r)\, m \in G$ $[\because -r$ is also an integer$]$

Also $(-r)\, m + r\, m = (-r + r)\, m = 0\, m = 0$

and $r\, m + (-r)\, m = (r - r)\, m = 0.$

$\therefore$ $(-r)\, m$ is the additive inverse of $r\, m$.

Thus every element of G possesses additive inverse.

Hence G is a group with respect to addition.

(iii) The set **N** of natural numbers is closed with respect to addition as well as with respect to multiplication. Therefore both addition and multiplication are binary operations on the set **N**. Also both addition and multiplication of natural numbers are associative operations.

Hence both the algebraic structures $(\mathbf{N}, +)$ and $(\mathbf{N}, \bullet)$ are semi-groups.

But the algebraic structure $(\mathbf{N}, +)$ is not a group because it does not possess identity element. There exists no natural number $e \in \mathbf{N}$ such that $e + a = a = a + e \ \forall\ a \in \mathbf{N}$. For the addition of numbers, the number 0 is the identity and $0 \approx \mathbf{N}$. Therefore $(\mathbf{N}, +)$ is not a group.

Again the algebraic structure $(\mathbf{N}, \bullet)$ is also not a group. This algebraic structure possesses identity element and it is the natural number 1. We have $1a = a = a1 \forall a \in \mathbf{N}$. But except 1 no other natural number possesses multiplicative inverse. Hence $(\mathbf{N}, \bullet)$ is not a group.

Problem 4: *Show that the set of vectors defined as directed line segments does not form a group*

(i) with respect to scalar (dot) product *(ii) with respect to vector (cross) product.*

Solution: Let V denote the set of all vectors defined as directed line segments.

(i) If $\mathbf{a}, \mathbf{b} \in V$, then $\mathbf{a} \bullet \mathbf{b}$ is a scalar quantity and so $\mathbf{a} \bullet \mathbf{b} \approx V$. Thus dot product of vectors is not a binary operation on the set V. Hence V cannot be a group with respect to dot product.

(ii) If $\mathbf{a}, \mathbf{b} \in V$, then the cross product $\mathbf{a} \times \mathbf{b}$ is also a vector and so $\mathbf{a} \times \mathbf{b} \in V$. Thus cross product of two vectors is a binary operation on the set V. But the cross product of vectors is not an associative operation. If $\mathbf{a}, \mathbf{b}, \mathbf{c} \in V$, then in general

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) \neq (\mathbf{a} \times \mathbf{b}) \times \mathbf{c}.$$

Hence V is not a group with respect to cross product.

Problem 5: *(i) Is the set of all non-negative integers with operation '+' a group? Justify your answer.*

(ii) Does the set of all odd integers form a group with respect to addition?

(Kumaun 2008, 11, 14)

Solution: (i) No. Except 0 no other non-negative integer possesses additive inverse.

(ii) We know that the sum of two odd integers is an even integer. For example $3 + 7 = 10$ which is even. Therefore the set of odd integers is not closed with respect to addition. Thus addition is not a binary composition in the set of odd integers. Therefore the question of the set of odd integers becoming a group with respect to addition does not arise.

Problem 6: *Is the set* $\mathbf{I}$ *of integers* $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ *a group*

(i) with respect to subtraction ? *(ii) with respect to multiplication ?*

Solution: (i) We have $a - b \in \mathbf{I} \quad \forall\, a, b \in \mathbf{I}$. Therefore $\mathbf{I}$ is closed with respect to subtraction. But subtraction in $\mathbf{I}$ is not an associative composition. For example,

$$(7 - 3) - 2 = 4 - 2 = 2, \quad 7 - (3 - 2) = 7 - 1 = 6.$$

Thus $(7 - 3) - 2 \neq 7 - (3 - 2)$. Therefore $(\mathbf{I}, -)$ is not a group.

(ii) We have $ab \in \mathbf{I} \,\forall\, a, b \in \mathbf{I}$. Therefore $\mathbf{I}$ is closed with respect to multiplication. Also multiplication of integers is an associative composition. The integer 1 is the multiplicative identity since $1a = a = a1 \;\forall\, a \in \mathbf{I}$. But 1 and -1 are the only integers which possess multiplicative inverse. Inverse of 1 is 1 and the inverse of -1 is -1. However $2 \in \mathbf{I}$ and the inverse of 2 for multiplication would have been 1/2 which is not an element of $\mathbf{I}$. Therefore $\mathbf{I}$ is not a group with respect to multiplication.

Problem 7: *Show that the set of all positive rational numbers forms an abelian group under the composition defined by* $a * b = (ab)/3$.

(Meerut 2004B, 09B; Bundelkhand 05; Avadh 09)

Solution: Let $\mathbf{Q}_+$ denote the set of all positive rational numbers. We define an operation $*$ on $\mathbf{Q}_+$ as follows :

$$a * b = (ab)/3 \quad \forall\, a, b \in \mathbf{Q}_+ .$$

To show that $(\mathbf{Q}_+, *)$ is a group.

Closure property: Since for every $a, b \in \mathbf{Q}_+$, $(ab)/3$ is also in $\mathbf{Q}_+$, therefore $\mathbf{Q}_+$ is closed with respect to the operation $*$.

Associativity: Let $a, b, c \in \mathbf{Q}_+$. Then

$$(a * b) * c = \left(\frac{ab}{3}\right) * c = \frac{[(ab)/3]\,c}{3}$$

$$= \frac{a\,[(bc)/3]}{3} = a * \left(\frac{bc}{3}\right) = a * (b * c).$$

Commutativity: Let $a, b \in \mathbf{Q}_+$. Then $a * b = (ab)/3 = (ba)/3 = b * a$.

Existence of Identity: The number e will be the identity element if $e \in \mathbf{Q}_+$ and if

$$e * a = a = a * e \quad \forall\, a \in \mathbf{Q}_+.$$

Now $e * a = a \Rightarrow (ea)/3 = a \Rightarrow (a/3)(e - 3) = 0 \Rightarrow e = 3,$

since $a \in \mathbf{Q}_+ \Rightarrow a \neq 0.$

Now $3 \in \mathbf{Q}_+$ and we have $3 * a = (3a)/3 = a = a * 3 \;\forall\; a \in \mathbf{Q}_+$.

$\therefore$ 3 is the identity element.

Existence of Inverse: Let a be any element of $\mathbf{Q}_+$. If the number b is to be the inverse of a, then we must have

$$b * a = e = 3 \quad \Rightarrow \quad (ba)/3 = 3 \Rightarrow b = 9/a.$$

Now $a \in \mathbf{Q}_+ \quad \Rightarrow \quad 9/a \in \mathbf{Q}_+$.

We have $(9/a) * a = \{(9/a)a\}/3 = 3 = a * (9/a)$.

Therefore $9/a$ is the inverse of a. Thus each element of $\mathbf{Q}_+$ is inversible.

Hence $(\mathbf{Q}_+, *)$ is an abelian group.

Problem 8: *Let* $\mathbf{R}$ *be the set of all real numbers and* $*$ *a binary operation on* $\mathbf{R}$ *defined by* $a * b = a + b + ab$. *Determine the identity element in* $\mathbf{R}$ *and determine the inverse of a.*

Solution: Let R be the set of all real number and $*$ a binary operation or R defined by

$$a * b = a + b + ab.$$

Let $e \in R$.

Then e will be the identity iff $\forall\; a \in R$

We have $e * a = a \quad \Rightarrow \quad e + a + ea = a$

$\Rightarrow \quad e + ae = 0 \quad \Rightarrow \quad e(1 + a) = 0$

$\Rightarrow \quad e = 0$ [Note that $a \in R \Rightarrow a \neq -1$]

$\therefore$ Identity element is 0 if $a \neq -1$

Let $a \in R$. Now $b \in R$ will be inverse of a if $b * a = 0$

$\Rightarrow \quad b + a + ba = 0 \quad \Rightarrow \quad b(a + 1) = -a$

$\Rightarrow \quad b = \dfrac{-a}{a+1}.$

Then $a^{-1} = b = -\dfrac{a}{a+1}$ is the inverse of a.

Problem 9: *Show that the set of all rational numbers of the form* $2^a\ 3^b$ $(a, b$ *integers*$)$ *is a group with respect to multiplication of rationals.*

Solution: Do yourself. Here rational number $2^0.3^0$, *i.e.*, 1 is the multiplicative identity. Also the rational number $2^{-a}\ 3^{-b}$ is the multiplicative inverse of $2^a\ 3^b$.

Problem 10: *Do the positive irrationals form a group with respect to multiplication?*

Solution: No. The set of positive irrationals is not closed for multiplication. For example, $\sqrt{2}\ .\ \sqrt{2} = 2$ which is a rational number and so it does not belong to the set of positive irrationals.

Problem 11: *Show that the set of positive rational numbers does not form a group with respect to the binary operation $*$ defined by $a * b = a/b$.*

Solution: The set $\mathbf{Q}_+$ of positive rational numbers is closed for the operation $*$. If $a, b \in \mathbf{Q}_+$, then $a * b = a/b$ is also a positive rational number and so $a * b \in \mathbf{Q}_+$.

But the operation on $\mathbf{Q}_+$ defined by $*$ is not associative. If $a, b, c \in \mathbf{Q}_+$, then in general

$$(a/b)/c = a/(b/c)$$

Hence $(\mathbf{Q}_+, *)$ is not a group.

Comprehensive Problems 2

Problem 1: *Distinguish between an abelian and a non-abelian group. Give an example of each.*

Solution: **Abelian Group:** Let $(G. *)$ be an algebraic structure, If G satisfies closure axiom, associative axiom, identity axiom, inverse axiom and commutative axiom with binary operation $*$, then G is an Abelian Group under the operation $*$.

Non-Abelian Group: A non abelian group is that group which does not satisfy commutative axiom.

Examples: 1. The set of all integers is an abelian group with respect to the operation of addition of integers.

2. The set of all $n \times n$ non-singular matrices having their elements as rational (real or complex) numbers is an infinite non-abelian group with respect to matrix multiplication.

Problem 2: *Show that the set $G = (...., 3^{-4}, 3^{-3}, 3^{-2}, 3^{-1}, 1, 3, 3^2, 3^3, 3^4, ...)$ forms an infinite abelian group with respect to multiplication.*

Solution: **Closure property:** Let a, b be any two elements of G

Then $a = 3^r$ and $b = 3^s$ were r and s are some integers.

Now $ab = 3^r 3^s = 3^{r+s} \in G$. Since $r + s$ is also some integer.

$\therefore$ G is closed with respect to multiplication.

Associativity : The elements of G are all rational numbers and the multiplication of rational numbers is associative.

Existence of left identity : We have $1 \in G$. Let a is any element of G.

Then $1a = a$. Therefore 1is the left identify

Existence of left inverse: We have $a \in G \Rightarrow a = b^r$ where r is some integer.

Now $3^r \in G \Rightarrow 3^{-r} \in G$ since $-r$ is also some integer.

We have $3^{-r}3^r = 3^0 = 1$. Therefore 3^{-r} is the left inverse of 3^r.

Commutativity: The multiplication of rational numbers is commutative.

Also the set G contains an infinite number of elements.

$\therefore$ G is an infinite abelian group with respect to multiplication.

Problem 3: *Show that the set* $\mathbf{I}$ *of all integers is an abelian group with operation defined by*

$$a * b = a + b + 2.$$ **(Meerut 2010, 12B; Kashi13)**

Solution: **Closure Property:** We have $a \in I, b \in I \Rightarrow a + b + 2 \in I$ *i.e.* $a * b \in I$.

Therefore I is closed with respect to the operation $*$.

Associativity: If $a, b, c \in I$, then

$$(a * b) * c = (a + b + 2) * c = a + b + 2 + c + 2$$
$$= a + b + c + 4$$

Also
$$a * (b * c) = a * (b + c + 2) = a * (b + c + 2)$$
$$= a + b + c + 4$$

$\therefore$ $(a * b) * c = a * (b * c)\ \forall\ a,b,c \in I$.

Existence of left identity: $e \in I$ will be the left identity of $e * a = a\ \forall\ a \in I$.

Now $e * a = e + a + 2$

$\therefore$ $e + a + 2 = a \Rightarrow e = -2$

Since $-2 \in I$ and we have for any $a \in I$.

Problem 4: *Prove that the set of rational numbers of the from* $m / 2^n$ *(*m, n *integers) is a group under addition.*

Solution: Let $G = \left\{ \frac{m}{2^n} :\ m, n \in I \right\}$.

Closure property: We know that the addition of rational numbers is also a rational number.

Therefore G is closed with respect to addition.

Associativity: We know that addition of rational numbers is an associative composition.

Existence of Left Identity: We have $\frac{0}{2^0} \in G$, since $0 \in I$. If $\frac{m}{2^n}$ is any element of G, then

$$\frac{0}{2^0} + \frac{m}{2^n} = \frac{0.2^n + m.2^0}{2^0\, 2^n} = \frac{m}{2^n}.$$

$\therefore$ $\frac{0}{2^0}$ is the left identity.

Existence of Left Inverse: We have

$$\frac{m}{2^n} \in G \ \Rightarrow\ \frac{(-m)}{2^{(-n)}} \in G \ \text{ since } m,n \in I \ \Rightarrow\ -m, -n \in I$$

Now $\frac{(-m)}{2^{(-n)}} + \frac{m}{2^n} = \frac{0}{2^0} = 0 =$ the left identity

$\therefore$ $\frac{(-m)}{2^{(-n)}}$ is the left inverse of $\frac{m}{2^n}$.

Hence G is a group with respect to addition.

Problem 5: *Show that the set G of all square matrices* $[a_{ij}]_{n\times n}$ *such that det* $[a_{ij}] = \pm 1$ *is a group under matrix multiplication. Show also that all those matrices in G for which det* $[a_{ij}] = 1$ *form a group.*

Solution: Write the complete proof yourself.

Here if $A, B \in G$, then det $A = \pm 1$ and det $B = \pm 1$.

We have det $(AB) = (\det A) . (\det B) = \pm 1$ and so $AB \in G$.

If I is unit matrix of order n, then det $I = 1$ and so $I \in G$.

If $A \in G$, then det $A = \pm 1$. Since det $A \neq 0$, therefore the matrix A is non-singular and so is invertible. If B is the inverse of A, then

$$AB = I \Rightarrow \det(AB) = \det I$$

$$\Rightarrow \quad (\det A) . (\det B) = 1$$

$$\Rightarrow \quad \det B = \pm 1, \text{ because det } A = \pm 1.$$

Thus $A \in G \Rightarrow A^{-1} = B \in G$. Thus each member of G has its inverse in G.

Hence G is a group for matrix multiplication.

Similarly we can show that all those matrices in G for which det $[a_{ij}] = 1$ also form a group.

Problem 6: *(i) If G is a group and* $a \in G$ *is such that* $aa = a$, *prove that* $a = e$.

(ii) If every element of a group is its own inverse, show that the group must be abelian.

(Bundelkhand 2005, 06, 10; Purvanchal 08; Avadh 13)

Solution: (i) We have $aa = a$

$$\Rightarrow \quad aa = ae \qquad [\because \ ae = a, e \text{ being the identity of } G]$$

$$\Rightarrow \quad a = e, \text{ by left cancellation law in } G.$$

(ii) Let a and b be any two elements of G. Then ab is also an element of G. Therefore $(ab)^{-1} = ab$ as it given that every element of G is its own inverse.

Now $\quad (ab)^{-1} = ab \Rightarrow b^{-1} a^{-1} = ab$

$$\Rightarrow \quad ba = ab. \qquad [\because \ a^{-1} = a, b^{-1} = b]$$

Thus we have $ab = ba \ \forall \ a, b \in G$. Hence G is an abelian group.

Problem 7: *(i) Show that the set of all matrices* $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, *a and b being non-zero reals, is a group under matrix multiplication.*

(ii) Show that the set of all matrices $\begin{bmatrix} c^{a} & b \\ 0 & c^{-a} \end{bmatrix}$, *a and b real, is a group under matrix multiplication, c being a positive constant.*

(iii) Show that the set of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, *where a and b are real numbers not both equal to zero, is a group under matrix multiplication.*

Solution: (i) Proceed as in part (iii) of this problem.

(ii) Proceed as in part (iii) of this problem.

(iii) Let G denote the set of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where a and b are real numbers not both equal to zero.

Closure property: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be any two members of G. Then a and b are real numbers not both equal to zero. Also c and d are real numbers not both equal to zero.

We have $$AB = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{bmatrix}$$

$$= \begin{bmatrix} p & q \\ -q & p \end{bmatrix}, \text{ where } p = ac - bd \text{ and } q = ad + bc.$$

Obviously p and q are real numbers and they cannot be both equal to zero as shown below.

We have $\det A = a^2 + b^2 \neq 0$ and $\det B = c^2 + d^2 \neq 0$.

Also $\det (AB) = p^2 + q^2$.

But $\det (AB) = (\det A).(\det B)$.

$\therefore$ $\det A \neq 0$ and $\det B \neq 0 \Rightarrow \det (AB) \neq 0 \quad \Rightarrow \quad p^2 + q^2 \neq 0$

$\Rightarrow$ at least one of p and q is not zero.

Thus p and q are real numbers not both equal to zero.

$\therefore$ $A, B \in G \quad \Rightarrow \quad AB \in G$.

Hence the set G is closed for matrix multiplication.

Associativity: We know that matrix multiplication is associative.

Existence of identity: The unit matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is obviously a member of the set G because it is obtained by putting $a = 1$ and $b = 0$. We have

$$\boldsymbol{IA = A = AI, \ \forall A \in G.}$$

$\therefore$ the unit matrix I is the identity.

Existence of inverse: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ be any member of the set G. Then a and b are real numbers not both equal to zero.

We have $\det A = a^2 + b^2 \neq 0$. Therefore the matrix A is non-singular and is therefore invertible. We must show that $A^{-1} \in G$. Let $\det A = m$. Then m is a real number and $m > 0$.

We have

$$A^{-1} = \frac{1}{\det A}\text{adj } A = \frac{1}{m}\begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} a/m & -b/m \\ b/m & b/m \end{bmatrix}$$

which is obviously a member of the set G because at least one of $\frac{a}{m}$ and $\frac{-b}{m}$ is not equal to zero. Thus each member of G has its inverse in G.
Hence G is a group for matrix multiplication.

Problem 8: *Show that the following sets form groups with respect to the binary operation * defined on them as follows:*

(*i*) *the set* $\mathbf{Q}_1$ *of all rational numbers other than* 1, *with the operation defined by*

$$a * b = a + b - ab.$$ **(Rohilkhand 2006)**

(*ii*) *the set* $\mathbf{Q}'$ *of all rational numbers other than* -1, *with the operation defined by*

$$a * b = a + b + ab.$$ **(Bundelkhand 2009; Kashi 12)**

Solution: (i) **Closure Property.** Let $a, b \in \mathbf{Q}_1$. Then a and b are rational numbers such that

$$a \neq 1, b \neq 1.$$

Now $a * b = a + b - ab$ which is also a rational number and it cannot be equal to 1, since $a + b - ab = 1 \Rightarrow a + b - ab - 1 = 0 \Rightarrow (a - 1)(1 - b) = 0$

$$\Rightarrow a = 1 \text{ or } b = 1 \text{ which is not so.}$$

$\therefore$ $a * b \in \mathbf{Q}_1$ $\forall$ $a, b \in \mathbf{Q}_1$. Hence $\mathbf{Q}_1$ is closed with respect to the given composition.

Associativity: If $a, b, c \in \mathbf{Q}_1$, then

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)\, c$$
$$= a + b + c - ab - ac - bc + abc.$$

Also $$a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a\,(b + c - bc)$$
$$= a + b + c - ab - ac - bc + abc.$$

$\therefore$ $$a * (b * c) = (a * b) * c \quad \forall \; a, b, c \in \mathbf{Q}_1.$$

Existence of left Identity: Let $e \in \mathbf{Q}_1$, *i.e.*, let e be a rational number and $e \neq 1$. Then e will be the left identity iff $\forall\, a \in \mathbf{Q}_1$ we have

$$e * a = a \Leftrightarrow e + a - ea = a \Leftrightarrow e - ea = 0$$
$$\Leftrightarrow e\,(1 - a) = 0 \Leftrightarrow e = 0. \qquad [\text{Note that } a \in \mathbf{Q}_1 \Rightarrow a \neq 1]$$

Now $0 \in \mathbf{Q}_1$; so 0 is the left identity.

Existence of left Inverse: Let $a \in \mathbf{Q}_1$, *i.e.*, let a be a rational number and $a \neq 1$. Now $b \in \mathbf{Q}_1$ will be the left inverse of a iff $b * a = 0 \Leftrightarrow b + a - ba = 0 \Leftrightarrow b\,(a - 1) = a \Leftrightarrow b = \frac{a}{a - 1}$, since $a \neq 1$. Now $\frac{a}{a - 1}$ is definitely a rational number. Also $\frac{a}{a - 1}$ cannot be equal to 1. Therefore $\frac{a}{a - 1} \in \mathbf{Q}_1$ and so it is the left inverse of a.

Also $$a * b = a + b - ab = b + a - ba = b * a.$$

$\therefore$ The set $\mathbf{Q}_1$ of all rational numbers except 1 is an infinite abelian group with respect to the given composition.

(ii) Proceed as in part (i). Here 0 is the identity element and the inverse of a is $-\frac{a}{a + 1}$ which exists since $a + 1 \neq 0$ and $-\frac{a}{a + 1} \neq -1$.

Problem 9 : *(i) Show that the set of all complex numbers of the form* $\cos\theta + i\sin\theta$, *where* θ *is any real number, forms a group with respect to the operation of multiplication of complex numbers.*

(ii) Show that the set M of complex numbers z with the condition $|z| = 1$ *forms a group with respect to the operation of multiplication of complex numbers.*

Solution: (i) Let $G = \{z : z = \cos\theta + i\sin\theta, \theta \in \mathbf{R}\}$. Here $\mathbf{R}$ denotes the set of real numbers.

Write the complete solution yourself. For closure property, if

$z_1 = \cos\theta_1 + i\sin\theta_1$ and $z_2 = \cos\theta_2 + i\sin\theta_2$ be any two members of G, then

$$z_1 z_2 = (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)$$

$$= \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)$$

which is also a member of G because $\theta_1, \theta_2 \in \mathbf{R} \Rightarrow \theta_1 + \theta_2 \in \mathbf{R}$.

Multiplication of complex numbers is associative.

The complex number $\cos 0 + i\sin 0 = 1$ is a member of G and is the multiplicative identity.

If $z = \cos\theta + i\sin\theta$ is any member of G, then

$$\cos(-\theta) + i\sin(-\theta) = \cos\theta - i\sin\theta$$

is also a member of G because $\theta \in \mathbf{R} \Rightarrow -\theta \in \mathbf{R}$.

We have $(\cos\theta + i\sin\theta)(\cos\theta - i\sin\theta) = \cos^2\theta + \sin^2\theta = 1$.

So $\cos\theta - i\sin\theta$ is the multiplicative inverse of $\cos\theta + i\sin\theta$.

Hence G is a group for multiplication of complex numbers.

(ii) If $z = x + iy$ is a complex number, then

$$|z| = +\sqrt{(x^2 + y^2)} \quad i.e., \quad |z|$$

is the non-negative value of the square root of $x^2 + y^2$.

Closure Property: Let $z_1, z_2 \in M$. Then $|z_1| = 1 = |z_2|$.

Since $|z_1 z_2| = |z_1||z_2| = 1$, therefore $z_1 z_2 \in M$. Therefore M is closed with respect to multiplication of complex numbers.

Associativity: We know that multiplication of complex numbers is associative.

Existence of left Identity: Since $|1 + i0| = 1$, therefore $1 + i0$ is an element of M. If $a + ib \in M$, we have $(1 + i0)(a + ib) = a + ib$. Therefore $1 + i0$ is the left identity.

Existence of left Inverse: Let $z = a + ib \in M$. Then $|z| = 1$. Since z is a non-zero complex number, therefore its multiplicative inverse $\frac{1}{z}$ exists. Let $u = \frac{1}{z}$. Then $|u| = \left|\frac{1}{z}\right| = \frac{1}{|z|} = \frac{1}{1} = 1$. Therefore $u \in M$ and we have $uz = \frac{1}{z}.z = 1$. Thus u is the left inverse of z.

$\therefore$ M is a group with respect to multiplication of complex numbers.

Problem 10: *Show that the set V of all vectors (defined as directed line segments) forms an infinite abelian group with vector addition as composition.* **(Kanpur 2011)**

Solution: We know that the sum of two vectors is also a vector. Therefore V is closed with respect to addition of vectors. Also the vector addition is associative. If $\mathbf{0}$ is the zero vector, then $\mathbf{0} \in V$ and we have $\mathbf{0} + \mathbf{a} = \mathbf{a} = \mathbf{a} + \mathbf{0} \ \forall\, \mathbf{a} \in V$.

Therefore the vector $\mathbf{0}$ is the identity element.

If $\mathbf{a} \in V$, then $-\mathbf{a} \in V$ and we have

$$-\mathbf{a} + \mathbf{a} = \mathbf{0} = \text{the identity element} = \mathbf{a} + (-\mathbf{a}).$$

Therefore $-\mathbf{a}$ is the inverse of $\mathbf{a}$.

Also vector addition is commutative.

$\therefore$ V is an infinite abelian group with respect to addition of vectors.

Problem 11: *Show that the set $\mathbf{C}_0$ of all non-zero complex numbers is a group with respect to multiplication of complex numbers.*

Solution: We have $\mathbf{C}_0 = \{a + ib : a \in \mathbf{R}, b \in \mathbf{R}$ and a and b are not both equal to $0\}$. The number $0 + i\,0$ is the zero complex number.

Closure property: We know that the product of two non-zero complex numbers is also a non-zero complex number. Therefore $\mathbf{C}_0$ is closed with respect to multiplication.

Associativity: We know that multiplication of complex numbers is associative.

Existence of left Identity: We have $1 + i0 \in \mathbf{C}_0$ since $1 + i0$ is a non-zero complex number.

Also if $a + ib \in \mathbf{C}_0$, then $(1 + i\,0)(a + ib) = a + ib$.

$\therefore$ $1 + i0$ is the left identity.

Existence of left Inverse: Let $a + ib \in \mathbf{C}_0$ *i.e.*, $a \in \mathbf{R}$, $b \in \mathbf{R}$ and a and b are not both equal to zero. Let $x + iy$ be the left inverse of $a + ib$. Then $(x + iy)(a + ib) = 1 + i\,0$

$$\Rightarrow \quad (xa - yb) + i\,(xb + ya) = 1 + i\,0$$

$$\Rightarrow \quad xa - yb = 1,\ xb + ya = 0.$$

Solving the equations $xa - yb = 1,\ xb + ya = 0$, we get

$$x = \frac{a}{a^2 + b^2},\ y = \frac{-b}{a^2 + b^2}.$$

Since $a^2 + b^2 \neq 0$ and a and b are not both equal to zero, therefore x and y are real numbers not both equal to zero. Therefore $\dfrac{a}{a^2 + b^2} + i\left(\dfrac{-b}{a^2 + b^2}\right) \in \mathbf{C}_0$ and it is the multiplicative left inverse of $a + ib$.

$\therefore$ $\mathbf{C}_0$ is a group with respect to multiplication.

Since multiplication of complex numbers is commutative, therefore the group is an abelian group.

Problem 12: *Show that the set of complex numbers z with $|z| = 1$ is not a group under the operation $*$ defined by $z_1 * z_2 = |z_1|\, z_2$.*

Solution: Proceed as in problem 9(ii).

Comprehensive Problems 3

Problem 1: *Show that the set* $G = \{1, -1\}$ *is a finite abelian group of order* 2 *under multiplication as composition.*

Solution: Proceed as in example 10, after article 9.

Problem 2: *Show that the set* $G = \{1, \omega, \omega^2\}$, *where* ω *is an imaginary cube root of unity is a group with respect to multiplication.* **(Garhwal 2001; Bundelkhand 06)**

Solution: We form the composition table:

Multiplication	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Note that
$\omega\omega^2 = \omega^3 = 1$ and
$\omega^2\omega^2 = \omega^4 = \omega^3\omega$
$= 1\omega$
$= \omega$

1. Since all the entries in the composition table are elements of the set G, therefore G is closed with respect to multiplication.
2. The elements of G are complex numbers and we know that multiplication of complex numbers is associative.
3. From the composition table we see that

$$1\,(1) = 1, \quad 1\,(\omega) = \omega = \omega\,(1),\ 1\,(\omega^2) = \omega^2 = \omega^2\,(1).$$

Therefore 1 is the identity element.

4. The inverses of $1, \omega, \omega^2$ are $1, \omega^2, \omega$ respectively.
5. The multiplication of complex numbers is commutative.

The number of elements in the set G is 3.

Hence G is a finite abelian group of order 3.

Problem 3: *Show that the set of four transformations* f_1, f_2, f_3, f_4 *on the set of complex numbers defined by* $f_1(z) = z,\ f_2(z) = -z,\ f_3(z) = 1/z, f_4(z) = -1/z$ *forms a finite abelian group with respect to the composite composition.*

Solution: Let $G = \{f_1, f_2, f_3, f_4\}$.

Suppose we denote multiplicatively the composition known as the **composite** or **product** of two functions. If $f : A \to B$ and $g : B \to C$ then by definition $(g\,f) : A \to C$ such that $(g\,f)(x) = g[f(x)]\ \forall\ x \in A$. The function $g\,f$ is called the composite of the functions g and f. We prepare the composition table as follows :

Since the function f_1 is the identity function, therefore

$$f_1\,f_1 = f_1,$$
$$f_1\,f_2 = f_2 = f_2\,f_1,$$
$$f_1\,f_3 = f_3 = f_3\,f_1,$$
$$f_1\,f_4 = f_4 = f_4\,f_1.$$

Now $(f_2\ f_2)(z) = f_2[f_2(z)] = f_2(-z) = -(-z) = z = f_1(z)$

$(f_2\ f_3)(z) = f_2[f_3(z)] = f_2\left(\frac{1}{z}\right) = -\frac{1}{z} = f_4(z)$

$(f_2\ f_4)(z) = f_2[f_4(z)] = f_2\left(-\frac{1}{z}\right) = \frac{1}{z} = f_3(z).$

Similarly calculating the other products we get the following composition table :

Composite of two functions	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

We make the following observations :

1. All the entries in the composition table are elements of the set G, therefore G is closed with respect to the given composition.
2. We know that the composite of functions is an associative composition *i.e.*, if $f : A \to B,\ g : B \to C,\ h : C \to D$, then
   $h(g\ f) = (h\ g)\ f$.
3. The identity function f_1 is the identity element.
4. Each of the given functions possesses inverse. Thus
   $f_1^{-1} = f_1,\ f_2^{-1} = f_2,\ f_3^{-1} = f_3,\ f_4^{-1} = f_4$.
5. The composition is commutative since $f_2\ f_3 = f_4$ and $f_3\ f_2 = f_4$.

The set G contains 4 elements. Hence G is a finite abelian group of order four with respect to the composite composition.

Problem 4: *Show that the composition table for a finite group contains each group element once and only once in each of its rows and columns.*

Solution: Let $G = \{a_1, a_2, ..., a_n\}$ be a finite group of order n, the operation denoted multiplicatively.

Let $a_i \in G$. Then to show that in the composition table for G the row headed by a_i contains each element of G once and only once.

The respective elements in the row headed by a_i are the values of the n products $a_i\ a_1, a_i\ a_2, ..., a_i\ a_n$. By closure property all these n products are elements of the set G. Also no two of these n products can give the same element of G. For suppose $a_i\ a_j = a_i\ a_k$, where a_j, a_k are distinct elements of G.

Then by left cancellation law in G, we have $a_j = a_k$. But this is a contradiction since a_j, a_k are distinct.

Hence all the n products $a_i\ a_1, a_i\ a_2, ..., a_i\ a_n$ are distinct elements of G and so they are the n elements of G placed in some order. Therefore the row headed by a_i contains each element of G once and only once.

Similarly by considering the n products $a_1 a_i , a_2 a_i , ..., a_n a_i$ and using the right cancellation law in G, we can show that the column headed by a_i contains each element of G once and only once.

Problem 5: *Forming the composition table for the multiplicative group $\{e, a, b\}$ of order 3, show that every group of order 3 must be abelian.*

Solution: Let $G = \{e, a, b\}$ be a multiplicative group of order 3, e being the identity element of the group. We shall form the composition table for G keeping in the mind the fact that the composition table for a finite group contains each group element once and only once in each of its rows and columns.

Composition table for G

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Since e is the identity, therefore the respective elements in the row headed by e are e, a and b and the respective elements in the column headed by e are e, a and b.

Now the product ab can be either equal to e or it can be equal to b.

We have $ab = b \Rightarrow ab = eb$

$\Rightarrow$ $a = e$, by right cancellation law in G.

But we have $a \neq e$. So ab cannot be equal to b and consequently be must have $ab = e$. Thus in the composition table we fill e at the place where the row headed by a and the column headed by b meet. Now the remaining entries of the composition table are easily filled by using the fact mentioned earlier. The complete composition table is as shown above. We observe that the corresponding rows and columns in the composition table are identical and so the composition in G is commutative. Hence G is an abelian group.

Comprehensive Problems 4

Problem 1: *Show that the relation 'congruence modulo m' is an equivalence relation in the set of integers and has m distinct equivalence classes.*

Solution: For complete solution of this problem refer theorem 1 of article 13.

Problem 2: *Is the set $\{1, 2, 3, 4, 5\}$ a group under (i) addition modulo 6, (ii) multiplication modulo 6 ?*

Solution: Let S denote the set $\{1, 2, 3, 4, 5\}$.

(i) We have $2 \in S, 4 \in S$ but $2 +_6 4 = 0 \notin S$. Thus S is not closed for addition modulo 6, *i.e.*, '$+_6$' is not a binary operation on the set S and so the question of S becoming a group under addition modulo 6 does not arise.

(ii) We have $2 \in S, 3 \in S$ but $2 \times_6 3 = 0 \notin S$ and so S is not closed for multiplication modulo 6. Hence S cannot be a group for multiplication modulo 6.

Problem 3: *Does the set of residue classes modulo 5 form a group with respect to addition?*

Solution: Let $G = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ be the set of residue classes modulo 5.

The composition table for G for addition of residue classes modulo 5 is as given below.

Addition	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Note that $\bar{1} + \bar{4} = \bar{5} = \bar{0}$

$\bar{2} + \bar{3} = \bar{5} = \bar{0}, \bar{2} + \bar{4} = \bar{6} = \bar{1},$

$\bar{3} + \bar{4} = \bar{7} = \bar{2}$, etc..

We see that all the entries in the composition table are elements of the set G. Therefore G is closed with respect to addition of residue classes modulo 5.

The composition of addition of residue classes is associative on the set G. For if $\bar{a}, \bar{b}, \bar{c}$ are any three elements of G, then

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b + c} = \overline{a + (b + c)} = \overline{(a + b) + c} = \overline{a + b} + \bar{c}$$
$$= (\bar{a} + \bar{b}) + \bar{c}.$$

Existence of identity: We have $\bar{0} \in G$. If $\bar{a}$ is any element of G, then $\bar{0} + \bar{a} = \overline{0 + a} = \bar{a} = \bar{a} + \bar{0}$. Therefore $\bar{0}$ is the identity.

Existence of inverse: From the table we see that the inverses of $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ are $\bar{0}, \bar{4}, \bar{3}, \bar{2}, \bar{1}$ respectively. For example $\bar{1} + \bar{4} = \bar{5} = \bar{0} = \bar{4} + \bar{1}$ implies that $\bar{1}$ and $\bar{4}$ are inverses of each other.

Hence, G is a group for addition of residue classes modulo 5.

Problem 4: *Prove that the set* $\{0, 1, 2, 3, 4\}$ *is a finite abelian group of order 5 under addition modulo 5 as composition.* **(Bundelkhand 2008)**

Solution: Let $G = \{0, 1, 2, 3, 4\}$.

Let us form the Composition table:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

We see that all the entries in the composition table are elements of the set G. Therefore G is closed with respect to addition modulo 5 *i.e.*, $+_5$.

The composition $+_5$ is **associative**. If a, b, c are any three elements of G, then

$$a +_5 (b +_5 c) = a +_5 (b + c)$$
$$= \text{least non-negative remainder when } a + (b + c) \text{ is divided by } 5$$
$$= \text{least non-negative remainder when } (a + b) + c \text{ is divided by } 5$$
$$= (a + b) +_5 c = (a +_5 b) +_5 c. \qquad [\because\ a + b = a +_5 b \ (\text{mod}5)]$$

Existence of identity: We have $0 \in G$. If a is any element of G, then from the composition table we see that $0 +_5 a = a = a +_5 0$.
There 0 is the identity element.

Existence of inverse : From the table we see that the inverses of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively. For example

$$4 +_5 1 = 0 = 1 +_5 4 \Rightarrow 4 \text{ is the inverse of } 1.$$

The composition is commutative as the corresponding rows and columns in the composition table are identical.
The number of element in the set G is 5
$\therefore$ $(G, +_5)$ is a finite abelian group of order 5.

Problem 5: *Prove that the set* $\{1, 2, 3, 4\}$ *is a finite abelian group of order* 4 *under multiplication modulo* 5 *as composition.*

Solution: First form the composition table and then proceed as in Example 14. Here the inverses of 1, 2, 3, 4 are 1, 3, 2, 4 respectively. For example $2 \times_5 3 = 1 = 3 \times_5 2$ implies that 2 and 3 are inverses of each other. Also $4 \times_5 4 = 1$ implies that the inverse of 4 is 4 itself.

Problem 6: *Show that the set* $\{1, 3, 4, 5, 9\}$ *is an abelian group under multiplication modulo* 11 *as composition. What is the order of this group?*

Solution: Let G denote the set $\{1, 3, 4, 5, 9\}$. Let us form the composition table for G for multiplication modulo 11.

$\times_{11}$	1	3	4	5	9
1	1	3	4	5	9
3	3	9	1	4	5
4	4	1	5	9	3
5	5	4	9	3	1
9	9	5	3	1	4

We see that all the entries in the composition table are elements of the set G. Therefore G is closed with respect to '$\times_{11}$'.
The composition '$\times_{11}$' on the set G is **associative.** If a, b, c are any three elements of G, then

$$a \times_{11} (b \times_{11} c) = (a \times_{11} b) \times_{11} c \text{ because } a(bc) = (ab)c.$$

Existence of Identity: We have $1 \in G$. If a is any element of G, then from the composition table we see that

$$1 \times_{11} a = a = a \times_{11} 1.$$

$\therefore$ 1 is the identity element.

Existence of Inverse: From the table we see that the inverses of 1, 3, 4, 5, 9 are 1, 4, 3, 9, 5 respectively. For example

$$5 \times_{11} 9 = 1 = 9 \times_{11} 5$$

implies that 5 and 9 are inverses of each other.

The composition '$\times_{11}$' on the set G is commutative as the corresponding rows and columns in the composition table are identical. The set G has 5 elements. Hence $(G, \times_{11})$ is a finite abelian group of order 5.

Problem 7: *Prove that* $G = \{1, 5, 7, 11\}$ *is a group under multiplication modulo* 12.

Solution: Proceed as in example 15, after article 11. Here in this group each element is its own inverse.

Problem 8: *Which of the following sets are groups under multiplication modulo* 11 ?

(*i*) $\{1, 3, 5, 7, 8\}$, (*ii*) $\{1, 8\}$, (*iii*) $\{1, 10\}$.

Solution: (i) Let G denote the set $\{1, 3, 5, 7, 8\}$.

We have $3 \in G, 5 \in G$ but $3 \times_{11} 5 = 4 \notin G$. Thus G is not closed for multiplication modulo 11. Hence G cannot be a group for '$\times_{11}$'.

(ii) Let G denote the set $\{1, 8\}$.

We have $8 \in G, 8 \in G$ but $8 \times_{11} 8 = 9 \notin G$. Thus G is not closed for multiplication modulo 11. Hence G cannot be a group for '$\times_{11}$'.

(iii) Let G denote the set $\{1, 10\}$. The composition table for G for '$\times_{11}$' is given below.

$\times_{11}$	1	10
1	1	10
10	10	1

Now write the complete solution as in Example 15.

Here G is an abelian group of order 2 for '$\times_{11}$'. The identity of the group is 1 and each element of G is its own inverse. Note that $10 \times_{11} 10 = 1$ implies that the inverse of 10 is 10 itself.

Problem 9: *Define a semi-group and a group and prove that a semi-group G is a group if and only if the equations* $ax = b$ *and* $ya = b$ *have solutions in G for arbitrary* $a, b \in G$.

Solution: For definitions of semi-group and group refer articles 2 and 3.

'If part' of the question: Let G be a semi-group such that the equations $ax = b$ and $ya = b$ have solutions in G for arbitrary $a, b \in G$. Then to prove that G is a group. For complete proof of this portion refer article 16.

'Only if' part of the question: Let a semi-group G be a group. Then to prove that the equations $ax = b$ and $ya = b$ have solutions in G for arbitrary $a, b \in G$. For complete solution of this portion refer theorem 6 of article 5.

Comprehensive Problems 5

Problem 1: *Define the order of an element in (i) an additive group, (ii) a multiplicative group. What is the order of the residue class* [3] *in the multiplicative group of non-zero residue classes modulo* 5 ?

Solution: (i) Let $(G, +)$ be an additive group and let 0 denote the identity of this group.

By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that

$$na = a + a + a + \ldots + n \text{ times} = 0.$$

If there exists no positive integer n such that $na = 0$, then we say that a is of infinite order or of zero order.

(ii) Let G be a multiplicative group and let e denote the identity of this group.

By the order of an element $a \in G$ is meant the least positive integer n, if one exists, such that

$$a^n = aaa \ldots n \text{ times} = e.$$

If there exists no positive integer n such that $a^n = e$, then we say that a is of infinite order or of zero order.

Let $G = \{[1], [2], [3], [4]\}$ be the multiplicative group of non-zero residue classes modulo 5. The identity of this group is the residue class [1]. It is required to find the order of the residue class [3] in this group.

We have $[3]^1 = [3], [3]^2 = [3][3] = [9] = [4],$

$[3]^3 = [3]^2\,[3] = [4][3] = [12] = [2],$

$[3]^4 = [3]^3\,[3] = [2][3] = [6] = [1],$ *i.e.*, the identity of the group G.

Thus 4 is the least positive integer such that $[3]^4 = [1]$. Therefore $o([3]) = 4$.

Problem 2: *Distinguish between the order of a group and the order of an element in a group. Prove that if $a, x \in G$ then a and xax^{-1} have the same order in G.*

Solution: Let G be a finite group. Then by $o(G)$, *i.e.*, by the order of G we mean the number of distinct elements in the set G.

Again let G be any group and let a be any element of G. For the definition of the order of the element a see article 18.

To prove that $o(xax^{-1}) = o(a)$, proceed as in theorem 5 of article 18.

Problem 3: *Show that in a group G, we have $ab = e \Rightarrow a = b^{-1}$ and $b = a^{-1}$.*

Solution: We have

$$ab = e \Rightarrow a^{-1}(ab) = a^{-1}\,e \Rightarrow (a^{-1}a)\,b = a^{-1}$$

$\Rightarrow$ $\quad eb = a^{-1} \Rightarrow b = a^{-1}.$

Again $\quad ab = e \Rightarrow (ab)\,b^{-1} = eb^{-1} \Rightarrow a(bb^{-1}) = b^{-1}$

$\Rightarrow$ $\quad ae = b^{-1} \Rightarrow a = b^{-1}.$

Problem 4: *Show that in a group G, we have ab = a or ba = a ⇒ b = e, where e is the identity element of G.*

Solution: We have $ab = a \Rightarrow ab = ae$

$\Rightarrow$ $b = e$, by left cancellation law in G.

Again $ba = a \Rightarrow ba = ea$

$\Rightarrow$ $b = e$, by right cancellation law in G.

Problem 5: *Find the solution of the equation abxax = cbx in a group G, where a, b and c are given elements of G.*

Solution: Let a, b, c and $x \in G$ be such that $abxax = cbx$.

Then by right cancellation law in G, we have $abxa = cb$

$\Rightarrow$ $a^{-1}\, a\, bx\, aa^{-1} = a^{-1}\, cb\, a^{-1}$,

multiplying both sides on the right and the left by a^{-1}

$\Rightarrow$ $e\, bx\, e = a^{-1}\, c\, ba^{-1} \quad \Rightarrow \quad bx = a^{-1}\, cb\, a^{-1}$

$\Rightarrow$ $b^{-1}\, bx = b^{-1}\, a^{-1}\, cba^{-1} \quad \Rightarrow \quad ex = b^{-1}\, a^{-1}\, cba^{-1}$

$\Rightarrow$ $x = b^{-1}\, a^{-1}\, cba^{-1}$.

Hence $x = b^{-1}\, a^{-1}\, cba^{-1}$ is the required solution of the given equation in the group G.

Problem 6: *If in a group G, the elements a and b commute, then prove that (i) a^{-1} and b^{-1} also commute, (ii) a^{-1} and b also commute, (iii) a and b^{-1} also commute.*

Solution: It is given that a and b commute, *i.e.*, $ab = ba$.

(i) We have $ab = ba \quad \Rightarrow \quad (ab)^{-1} = (ba)^{-1} \quad \Rightarrow \quad b^{-1}\, a^{-1} = a^{-1}\, b^{-1}$

$\Rightarrow$ a^{-1} and b^{-1} commute.

(ii) We have $ab = ba \quad \Rightarrow \quad a^{-1}\,(ab) = a^{-1}\,(ba) \quad \Rightarrow \quad (a^{-1}\, a)\, b = (a^{-1}\, b)\, a$

$\Rightarrow$ $eb = (a^{-1}\, b)\, a \quad \Rightarrow \quad b = (a^{-1}\, b)\, a \quad \Rightarrow \quad ba^{-1} = (a^{-1}\, b)\, aa^{-1}$

$\Rightarrow$ $ba^{-1} = (a^{-1}\, b)\, e \quad \Rightarrow \quad ba^{-1} = a^{-1}\, b \quad \Rightarrow \quad a^{-1}$ and b commute.

(iii) Proceed as in part (ii).

Problem 7: *Prove that if $a^2 = a, a \in G$, then $a = e$.*

Solution: We have $a^2 = a \quad \Rightarrow \quad aa = a$

$\Rightarrow$ $aa = ae$ $\qquad [\because \ ae = a]$

$\Rightarrow$ $a = e$. [By left cancellation law in G]

Problem 8: *In a group G prove that $e^n = e$ for any integer n.* **(Agra 2000)**

Solution: (i) $n = 0$. We have $e^0 = e$ [By definition]

(ii) $n > 0$. We have $e^1 = e$.

Suppose $e^k = e$, where k is any positive integer.

Then $e^{k+1} = e^k\, e = ee = e$.

$\therefore$ By mathematical induction $e^n = e$, where n is any positive integer.

(iii) $n < 0$. Let $n = -m$ where m is a positive integer.

Then $e^n = e^{-m} = (e^{-1})^m = e^m = e$, by case (ii).

Hence $e^n = e$ for any integer n.

Problem 9: *Prove that a group G is abelian if every element of G except the identity element is of order two.*

Solution: Identity element e is of order 1. But $e^2 = e$. Since every other element is of order two, therefore we have $a^2 = e \ \forall\, a \in G$.

Now proceed as in Example 20.

Problem 10: *If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.*

Solution: Let G be a group of even order $2n$, where n is a positive integer. We shall prove that G must have an element $a \neq e$ such that $a^{-1} = a$. We shall prove it by contradiction.

Suppose G has no element, other than the identity element e, which is its own inverse. Now in a group every element possesses a unique inverse. The identity element e is its own inverse. Further if b is the inverse of c, then c is the inverse of b. So excluding the identity element e, the remaining $2n - 1$ elements of G must be divided into pairs of two such that each pair consists of an element and its inverse. But we cannot do so because the odd integer $2n - 1$ is not divisible by 2. Hence our initial assumption is wrong.

So in G there is an element $a \neq e$ such that

$$a = a^{-1} \Rightarrow aa = a^{-1}\, a \Rightarrow a^2 = e.$$

Problem 11: *Find the order of each element of the group* $(\{0, 1, 2, 3, 4\}, +_5)$.

(Meerut 2010B)

Solution: The identity of the group $(\{0, 1, 2, 3, 4\}, +_5)$ is 0. Therefore

$$o\,(0) = 1.$$

Now $1\,(1) = 1, 2\,(1) = 1 +_5 1 = 2, 3\,(1) = 1 +_5 1 +_5 1 = 3,$

$4\,(1) = 1 +_5 1 +_5 1 +_5 1 = 4, 5\,(1) = 1 +_5 1 +_5 1 +_5 1 +_5 1 = 0$ (*i.e.*, identity element).

Thus 5 is the least positive integer such that 5 (1) = identity of the group.

$\therefore$ $o\,(1) = 5.$

Again $1\,(2) = 2, 2\,(2) = 2 +_5 2 = 4, 3\,(2) = 2 +_5 2 +_5 2 = 4 +_5 2 = 1,$

$4\,(2) = 2 +_5 2 +_5 2 +_5 2 = 1 +_5 2 = 3,$

$5\,(2) = 2 +_5 2 +_5 2 +_5 2 +_5 2 = 3 +_5 2 = 0$ (*i.e.*, identity element).

$\therefore$ $o\,(2) = 5.$

Since $1 +_5 4 = 0 = 4 +_5 1$ and $2 +_5 3 = 0 = 3 +_5 2$, therefore in the given group the inverse of 1 is 4 and that of 2 is 3.

$\therefore$ $o\,(4) = o\,(1) = 5$ and $o\,(3) = o\,(2) = 5.$

Hence in the given group $o\,(0) = 1$ and each other element is of order 5.

Problem 12: *Find the order of each element in the multiplicative group* $G = \{1, \omega, \omega^2\}$ *where* $\omega^3 = 1$.

Solution: The identity of the given multiplicative group

$G = \{1, \omega, \omega^2\}$ is 1. Therefore $o(1) = 1$.

Again $\omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1$. Thus 3 is the least positive integer such that $\omega^3 = 1$. Therefore $o(\omega) = 3$.

Finally, $(\omega^2)^1 = \omega^2, (\omega^2)^2 = \omega^4 = \omega^3 . \omega = 1 . \omega = \omega,$

$(\omega^2)^3 = \omega^6 = (\omega^3)^2 = 1^2 = 1$ (*i.e.*, identity of G).

$\therefore$ $o(\omega^2) = 3$.

Problem 13: *Show by means of an example that it is possible for the quadratic equation* $x^2 = e$ *to have more than two solutions in some group* G *with identity* e.

Solution: Consider the symmetric group P_3 of permutations of degree 3 on a set $S = \{1, 2, 3\}$ having three symbols 1, 2 and 3.

We have $P_3 = \{I, (12), (23), (31), (123), (132)\}$ where I is the identity permutation on the set S and is the identity element of the group P_3.

Let $I = f_1, (12) = f_2, (23) = f_3, (31) = f_4, (123) = f_5, (132) = f_6$.

We have $f_1^2 = I, f_2^2 = (12)(12) = I, f_3^2 = (23)(23) = I, f_4^2 = (31)(31) = I$.

Thus there are four elements in the group P_3 satisfying the equation $x^2 = e$. Hence it is possible for the quadratic equation $x^2 = e$ to have more than two solutions in some group G with identity e.

Problem 14: *If the elements* a, b *and* ab *of a group are each of order* 2, *prove that* $ab = ba$.

Solution: Let G be a group, the operation denoted multiplicatively and let e be the identity element of the group G.

Let $a, b \in G$ be such that $o(a) = 2, o(b) = 2$ and $o(ab) = 2$.

We have $o(a) = 2 \Rightarrow a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$.

Similarly $o(b) = 2 \Rightarrow b^{-1} = b$ and $o(ab) = 2 \Rightarrow (ab)^{-1} = ab$.

Now $(ab)^{-1} = ab \Rightarrow b^{-1} a^{-1} = ab \Rightarrow ba = ab$. This proves the required result.

Problem 15: *Give an example of an infinite group each element of which has a finite order.*

Solution: Let $G = \{z : z \in \mathbf{C}$ and $z^n = 1$ for some positive integer $n\}$ *i.e.*, let G be the union of all n, nth roots of unity where $n \in \mathbf{N}$.

For multiplication of complex numbers G is an infinite group. If $z \in G$, then by our definition of G, we have $z^n = 1$ (*i.e.*, identity of G) for some positive integer n and so z is of finite order. Thus G is an infinite group each element of which has a finite order.

Problem 16: *Let* $x \in G, x \neq e$. *Show that* $x \neq x^{-1}$ *if and only if the order of* x *is greater than two, where* G *is any group.*

Solution: Let $x \in G$ and $x \neq e$.

First assume that $x \neq x^{-1}$. Then to show that $o(x) > 2$.

Since $x \neq e$, therefore $o(x) \neq 1$.

Also $\quad x \neq x^{-1} \Rightarrow xx \neq x\,x^{-1} \Rightarrow x^2 \neq e \Rightarrow o(x) \neq 2.$

$\therefore$ If $x \neq x^{-1}$, then $o(x) > 2$.

Conversely suppose that $o(x) > 2$. Then to show that $x \neq x^{-1}$.

We have $\quad o(x) > 2 \Rightarrow x^2 \neq e \Rightarrow xx \neq e \Rightarrow x \neq x^{-1}$.

$\therefore$ If $o(x) > 2$, then $x \neq x^{-1}$.

Hence if $x \neq e$, then $x \neq x^{-1}$ if and only if the order of x is greater than two.

Problem 17: *If a is an element of a group, prove that the integral powers of a form a multiplicative group.*

Solution: Let G be a multiplicative group and let $a \in G$.

Let $H = \{a^r : r \in \mathbf{I}$, where $\mathbf{I}$ is the set of integers$\}$.

To show that H is a group for multiplication.

Closure property: Let $x = a^r$, $y = a^s$ be any two elements of H, where r and s are some integers.

We have $xy = a^r a^s = a^{r+s} \in H$ because $r + s$ is also some integer.

$\therefore$ H is closed for multiplication.

Associativity: Since $H \subseteq G$, therefore the operation which is associative on G must also be associative on H.

Existence of identity: We have $a^0 = e \in H$ and $xe = x = ex \ \forall \ x \in H$. Therefore the identity of G is also the identity of H.

Existence of inverse: Let $x = a^r$ be any element of H, where r is some integer. Then a^{-r} is also an element of H because $-r \in \mathbf{I}$.

We have $a^{-r} a^r = a^0 = e = a^r a^{-r}$.

$\therefore$ a^{-r} is the inverse of a^r and so each element of H has its inverse in H.

Hence H is a group for multiplication.

Problem 18: *Prove that a group G is abelian iff $(ab)^{-1} = a^{-1} b^{-1} \ \forall \ a, b \in G$.*

Solution: First assume that a group G is abelian.

Then to prove that $(ab)^{-1} = a^{-1} b^{-1} \ \forall \ a, b \in G$.

Let $a, b \in G$. Then G is abelian

$\Rightarrow \quad ab = ba \Rightarrow (ab)^{-1} = (ba)^{-1} \Rightarrow (ab)^{-1} = a^{-1} b^{-1}$.

$\therefore$ if G is abelian, then $(ab)^{-1} = a^{-1} b^{-1} \ \forall \ a, b \in G$.

Conversely suppose that $(ab)^{-1} = a^{-1} b^{-1} \ \forall a, b \in G$. Then to prove that G is abelian.

Let a, b be any two elements of G.

Then $\quad (ab)^{-1} = a^{-1} b^{-1} \Rightarrow [(ab)^{-1}]^{-1} = (a^{-1} b^{-1})^{-1}$

$\Rightarrow \quad ab = (b^{-1})^{-1} (a^{-1})^{-1} \Rightarrow ab = ba.$

Thus $ab = ba, \ \forall \ a, b \in G$ and so the group G is abelian.

Hence a group G is abelian iff $(ab)^{-1} = a^{-1} b^{-1}, \ \forall \ a, b \in G$.

Problem 19: *In a group if $ba = a^m b^n$, prove that the elements $a^m b^{n-2}$, $a^{m-2} b^n$, ab^{-1} have the same order.* **(Meerut 2010)**

Solution: We have $a^m b^{n-2} = a^m b^n b^{-2} = bab^{-2}$ $[\because\ ba = a^m b^n]$

$= bab^{-1} b^{-1} = (b^{-1})^{-1} (ab^{-1}) b^{-1}$.

Now we know that in a group $o(a) = o(x^{-1} ax)$, where a, x are any two elements of the group.

$\therefore$ $o(a^m b^{n-2}) = o[(b^{-1})^{-1} (ab^{-1}) b^{-1}] = o(ab^{-1})$. ...(1)

Further $a^{m-2} b^n = a^{-2} a^m b^n = a^{-2} ba = a^{-2} ba^{2-1} = a^{-2} ba^{-1} a^2$

$= (a^2)^{-1} (ba^{-1}) a^2$.

$\therefore$ $o(a^{m-2} b^n) = o[(a^2)^{-1} (ba^{-1}) a^2] = o(ba^{-1})$

$= o[(ba^{-1})^{-1}]$, since $o(a^{-1}) = o(a)$

$= o[(a^{-1})^{-1} b^{-1}] = o(ab^{-1})$. ...(2)

From (1) and (2), we get $o(a^m b^{n-2}) = o(ab^{-1}) = o(a^{m-2} b^n)$.

Problem 20: *If in the group G, $a^5 = e$, $aba^{-1} = b^2$ for $a, b \in G$, find $o(b)$.*

(Meerut 2009)

Solution: We have

$(ab a^{-1})^2 = ab a^{-1} ab a^{-1} = ab^2 a^{-1}$

$= aa ba^{-1} a^{-1}$ $[\because\ ab a^{-1} = b^2]$

$= a^2 ba^{-2}$.

$\therefore$ $(ab a^{-1})^4 = \{(aba^{-1})^2\}^2 = (a^2 ba^{-2})^2 = a^2 ba^{-2} a^2 ba^{-2}$

$= a^2 b^2 a^{-2} = a^2 ab a^{-1} a^{-2} = a^3 ba^{-3}$.

$\therefore$ $(a ba^{-1})^8 = \{(aba^{-1})^4\}^2 = (a^3 ba^{-3})^2 = a^3 ba^{-3} a^3 ba^{-3} = a^3 b^2 a^{-3}$

$= a^3 ab a^{-1} a^{-3} = a^4 ba^{-4}$.

$\therefore$ $(a ba^{-1})^{16} = \{(aba^{-1})^8\}^2 = (a^4 ba^{-4})^2$

$= a^4 ba^{-4} a^4 ba^{-4} = a^4 b^2 a^{-4}$

$= a^4 a ba^{-1} a^{-4} = a^5 ba^{-5}$

$= eb e$ $[\because\ a^5 = e$ and so $a^{-5} = e]$

$= b$.

Thus $(aba^{-1})^{16} = b$.

$\therefore$ $(b^2)^{16} = b$ $[\because\ ab a^{-1} = b^2]$

$\Rightarrow$ $b^{32} = b \Rightarrow b^{31} = e$.

Since $b^m = e \Rightarrow o(b) \mid m$, therefore $o(b) \mid 31$.

But 31 is a prime integer. Therefore $o(b) = 1$ or 31.

So if $b = e$, then $o(b) = 1$ and if $b \neq e$, then $o(b) = 31$.

Problem 21: *If the elements a, b of a group commute and o (a) = m, o (b) = n, where m and n are relatively prime, prove that o (ab) = mn.*

Solution: It is given that the two elements a and b of a group commute and $o(a) = m$, $o(b) = n$ with $(m, n) = 1$. Here (m, n) stands for the H.C.F. of m and n.

We have to prove that $o(ab) = mn$.

Let $o(ab) = k$.

Since a and b commute, we have

$$(ab)^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = e^n e^m = e\, e = e.$$

$\therefore$ $k \mid mn$. [See theorem 4 of article 18]

Again $(ab)^k = a^k b^k$, since a and b commute.

But $o(ab) = k \Rightarrow (ab)^k = e$.

From these it follows that $a^k b^k = e$.

$\therefore$ $a^k = (b^k)^{-1} \Rightarrow o(a^k) = o[(b^k)^{-1}] \Rightarrow o(a^k) = o(b^k)$.

[$\because$ in a group, $o(a) = o(a^{-1})$]

Now by the corollary of theorem 4 of article 18, we have

$$o(a^k) \mid o(a) \text{ and } o(b^k) \mid o(b) \quad i.e.,\ o(a^k) \mid m \text{ and } o(b^k) \mid n.$$

Since $o(a^k) = o(b^k)$, we see that either $o(a^k)$ or $o(b^k)$ divides both m and n and so it divides their H.C.F. $(m, n) = 1$. But then we must have $o(a^k) = o(b^k) = 1$, so that $a^k = e$, and $b^k = e$. Hence by theorem 4 of article 18, we have $m \mid k$ and $n \mid k$. But $(m, n) = 1$, *i.e.*, m and n are relatively prime. Therefore $m \mid k$ and $n \mid k \Rightarrow mn \mid k$. But we have already shown that $k \mid mn$.

$\therefore$ We have $k = mn$, *i.e.*, $o(ab) = mn$.

Problem 22: *S is a semi-group. If for all x, y ∈ S, $x^2 y = y = yx^2$, prove that S is an abelian group.*

Solution: Let x be any element of S. Then $x^2 = xx \in S$ because S is closed for multiplication. According to hypothesis, we have

$$x^2 y = y = yx^2, \ \forall\ y \in S.$$

$\therefore$ x^2 is identity element. If we denote this identity element by e, then we have

$$x^2 = e \ \forall\ x \in S.$$

Now $x^2 = e \Rightarrow xx = e \Rightarrow x = x^{-1}$.

Thus each element of S is its own inverse. Hence the semi-group S is a group because it possesses identity and also the inverse of each element.

Now to show that S is also abelian. Let $x, y \in S$. Then xy is also an element of S. Therefore $(xy)^{-1} = xy$ because each element of S is its own inverse.

Now $(xy)^{-1} = xy \Rightarrow y^{-1} x^{-1} = xy \Rightarrow yx = xy$. [$\because$ $x^{-1} = x$, $y^{-1} = y$]

Thus we have $xy = yx \ \forall\ x, y \in S$.

Hence S is an abelian group.

Hints to Objective Type Questions

Multiple Choice Questions

1. See example 3 after article 4.

2. The identity of the given group is 1. We have $\omega^2 . \omega = \omega^3 = 1$. So, the inverse of ω^2 is ω.

3. The identity of the group $(\{0, 1, 2, 3, 4\}, +_5)$ is 0.
We have

$$1\,(1) = 1, 2\,(1) = 1 +_5 1 = 2, 3\,(1) = 1 +_5 1 +_5 1 = 3,$$
$$4\,(1) = 1 +_5 1 +_5 1 +_5 1 = 4,\ 5\,(1) = 1 +_5 1 +_5 1 +_5 1 +_5 1 = 0.$$
$$\therefore \quad o\,(1) = 5.$$

4. See problem 21 of Comprehensive Problems 5.

5. See problem 1 of Comprehensive Problems 3.

6. See Theorem 4 of article 5.

7. See article 18, Theorem 2.

8. A non-empty set G with a binary operation is called a groupoid.

9. See article 4.

10. See article 2.

11. See article 2.

12. See Example 2, after article 4.

13. See Theorem 6 of article 5.

14. See article 1.

15. See Note 2 of Theorem 4 of article 5.

16. See Theorem 1 of article 5.

17. See Theorem 3 of article 5.

18. See Problem 20 of Comprehensive Problems 5.

19. See article 3.

20. See Problem 2 of Comprehensive Problems 3.

21. See Example 5.

22. Additive identity 0 does not exists in N.

23. See Problem 8 of Comprehensive Problems 1.

24. See Illustration 2 after article 18.

25. Same as Question 22 above.

26. See article 10.

27. See article 18.

28. See article 18, Theorem 3.

29. See Example 2, Note.

30. See Problem 5(ii) of Comprehensive Problems 1.

31. See Example 5.

Fill in the Blank(s)

1. See article 2.
2. See article 3.
3. See article 4.
4. The integer 0 is an even integer and we have $0 + a = a = a + 0, \ \forall \ \ a \in E$.

   So, in the group $(E, +)$, the identity element is 0.
5. Let e be the identity element. Then,

$$e \ o \ a = a = a \ o \ e \ , \ \ \forall \ \ a \in \mathbf{Q}_+ \ \ \Rightarrow \ \ \frac{ea}{3} = a \ \Rightarrow \ e = 3.$$

6. See article 5, Theorem 4.
7. We have,

$$\begin{aligned}(ab^{-1})^{-1} \ (ca^{-1})^{-1} \ c &= [(b^{-1})^{-1} \ a^{-1}] \ [(a^{-1})^{-1} \ c^{-1}] \ c \\ &= ba^{-1} \ a \ c^{-1} \ c \\ &= b \ (a^{-1} \ a) \ (c^{-1} \ c) = b \ e \ e = b.\end{aligned}$$

8. The number of distinct elements in the group is n. So, the order of the group is n.
9. See example 15 after article 11.
10. In a group,

$$o \ (g \ h \ g^{-1}) = o \ (h).$$

    See article 18, Theorem 5.

    Since $o \ (h) = 3$, therefore

$$o \ (g \ h \ g^{-1}) = o \ (h) = 3.$$

11. See example 19 after article 18.
12. See example 20 after article 18.

True or False

1. See article 4.
2. The identity for multiplication is 1. The rational number 0 does not possess multiplicative inverse. Hence **Q** is not a group with respect to multiplication.
3. See problem 5(ii) of Comprehensive Problems 1.
4. See article 5, Theorem 2.
5. See problem 6(ii) of Comprehensive Problems 2.
6. See problem 7 of Comprehensive Problems 4.
7. See problem 8 part (i) of Comprehensive Problems 4.
8. See Illustration 4 after article 18.
9. See article 5, Theorem 4.

❍❍❍

Chapter-4

Permutation Groups

Comprehensive Problems 1

Problem 1: *Write down all the permutations on three symbols a, b, c. Which of these permutations are even?*

Solution: Let $S = \{a, b, c\}$. There are 3 !, *i.e.*, 6 distinct permutations on the set S. If P_3 denotes the set of all these 6 permutations, then

$$P_3 = \{I \text{ (}i.e.\text{, identity permutation,) } (ab), (bc), (ca), (abc), (acb)\}.$$

Out of these 3 !permutations half are even permutations and these are I,(abc) and (acb).

Problem 2: *Define a permutation. If* $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *and* $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, *find AB and BA.*

Solution: For definition of a permutation refer article 1.

We have $$AB = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{identity permutation.}$$

Note that under the permutation A the image of 1 is 2 and then under the permutation B the image of 2 is 1. So the image of 1 under the permutation AB is 1. Similarly we write the images of other elements under the permutation AB.

Again $$BA = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$= \text{identity permutation.}$$

Problem 3: *If* $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *and* $g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, *then find* fg *and* gf.

Solution: $$fg = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Problem 4: *Find the inverse of each of the following permutations:*

(i) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ **(Kanpur 2006, 09; Avadh 13)**

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(iii) $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}$. **(Kanpur 2010, 12)**

Solution: (i) Let $f=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$.

To write the inverse of the permutation f, we form a permutation g by interchanging the two rows of f. Thus we write

$$g=\begin{pmatrix}1 & 3 & 4 & 2\\ 1 & 2 & 3 & 4\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}.$$

We have $$fg=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

= identity permutation

and $$gf=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

= identity permutation.

$\therefore$ $$f^{-1}=g=\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}.$$

(ii) Proceed as in part (i) of this question. The required inverse is

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix}.$$

(iii) Proceed as in part (i) of this question. The required inverse is

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 2 & 5 & 4\end{pmatrix}.$$

Problem 5: *Decompose the permutation* $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 6 & 5 & 2 & 4 & 3 & 1 & 7\end{pmatrix}$ *into transpositions.*

(Meerut 2007, 10, 10B)

Solution: Let us denote the given permutation by f. First expressing f as a product of disjoint cycles, we can write

$$f=(1\ 6)\,(2\ 5\ 3)\,(4)\,(7)$$

$$=(1\ 6)\,(2\ 5\ 3),$$

omitting cycles of length 1 as they represent identity permutation.

Now expressing the cycle (2 5 3) as a product of transpositions, we can write

$$(2\ 5\ 3)=(2\ 5)\,(2\ 3).$$

Hence $$f=(1\ 6)\,(2\ 5)\,(2\ 3).$$

Problem 6: *Examine whether the following permutations are even or odd.*

(i) $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&5&4&3&6&1&7&9&8\end{pmatrix}$. **(Meerut 2008)**

(ii) $\begin{pmatrix}1&2&3&4&5&6&7&8\\3&6&4&1&8&2&5&7\end{pmatrix}$. **(Avadh 2012)**

Solution: (i) Let us denote the given permutation by f. Expressing f as a product of disjoint cycles, we can write

$$f = (1\,2\,5\,6)\,(3\,4)\,(7)\,(8\,9)$$
$$= (1\,2\,5\,6)\,(3\,4)\,(8\,9),$$

omitting cycle of length 1 because it represents identity permutation.

Now expressing the cycle (1 2 5 6) as a product of transpositions, we can write

$$(1\,2\,5\,6) = (1\,2)\,(1\,5)\,(1\,6).$$

$$\therefore \quad f = (1\,2)\,(1\,5)\,(1\,6)\,(3\,4)\,(8\,9).$$

Thus f has been expressed as a product of transpositions. The number of transpositions in this product is 5 which is odd. Hence f is an odd permutation.

(ii) Proceed as in part (i). **Ans.** odd permutation.

Problem 7: *How many times* $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$ *be multiplied to itself to produce* $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$*?* **(Meerut 2009; Rohilkhand 09)**

Solution: Let us denote the given permutation by f.

We have $$f\,f = \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}.$$

Now $$f\,f\,f = f\,(f\,f)$$
$$= \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$$
$$= \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \text{identity permutation.}$$

Hence $f\,f\,f$ produces identity permutation *i.e.*, the given permutation be multiplied 3 times to itself to produce identity permutation.

Problem 8: *Find the order of the permutation* $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$.

Solution: Let P_4 be the symmetric group of all permutations on the set $S = \{1, 2, 3, 4\}$. The identity of this group is the identity permutation

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}.$$

Let f denote the permutation $\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$.

Then $$f^1 = f,\ f^2 = ff = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix},$$

$$f^3 = fff = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{pmatrix}$$

i.e., identity of the group P_4.

Thus 3 is the least positive integer such that f^3 = identity of the group P_4.

$\therefore$ $o(f) = 3$.

Problem 9: *Given that* $f = (1\,3\,2\,5)\,(1\,4\,3)\,(2\,5\,1)$ *is a permutation on five symbols. Express it as a product of disjoint cycles. Also find the inverse of f and express it as a product of disjoint cycles.*

Solution: Expressing f as a product of disjoint cycles, we can write

$$f = (1\,2)\,(3\,5\,4).$$

Now the product of disjoint cycles is commutative. Also if the elements a and b of a group G commute, then $(ab)^{-1} = a^{-1}b^{-1}$. All the 5 !permutations on five symbols form a group for composite of permutations as the operation.

$\therefore$ $$f^{-1} = [(1\,2)\,(3\,5\,4)]^{-1} = (1\,2)^{-1}\,(3\,5\,4)^{-1}$$

$$= (2\,1)\,(4\,5\,3)$$

$$= (1\,2)\,(3\,4\,5).$$

Problem 10: *Prove that a cycle containing an odd number of symbols is an even permutation whereas a cycle containing an even number of symbols is an odd permutation.*

Solution: Let $f = (a_1\,a_2\,a_3 \ldots a_n)$ be a cycle containing n symbols. We can write

$$f = (a_1\,a_2)\,(a_1\,a_3) \ldots (a_1\,a_n).$$

Thus f has been expressed as a product of $n-1$ transpositions. If n is odd, then $n-1$ is even and consequently in this case f is an even permutation. Again if n is even, then $n-1$ is odd and so in this case f is an odd permutation. Hence a cycle containing an odd number of symbols is an even permutation whereas a cycle containing an even number of symbols is an odd permutation.

Problem 11: *Show that the set G of four permutations I,* $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$ *and* $(1\,4)\,(2\,3)$ *on four symbols* 1, 2, 3, 4 *is an abelian group with respect to the permutation multiplication. (This group is known as the four group* V_4 *of Klein.)*

Solution: Let $I = f_1$, $(12)(34) = f_2$, $(13)(24) = f_3$, $(14)(23) = f_4$. First we prepare composition table for the set G for the operation of product of permutations. Since f_1 is identity permutation, therefore

$$f_1 f_1 = f_1,\ f_1 f_2 = f_2 = f_2 f_1\ ,\ f_1 f_3 = f_3 = f_3 f_1\ ,\ f_1 f_4 = f_4 = f_4 f_1.$$

Further $f_2 f_2 = (13)(24)(13)(24)$.

But $(24)(13) = (13)(24)$ because the product of disjoint cycles is commutative.

$\therefore$ $f_2 f_2 = (13)(13)(24)(24) = (I)(I) = I = f_1$.

Again $f_2 f_3 = (12)(34)(13)(24) = (14)(23)$, by actual calculation of the product of the four permutations

$= f_4$,

$f_2 f_4 = (12)(34)(14)(23) = (13)(24) = f_3$.

Similarly $f_3 f_2 = (13)(24)(12)(34) = (14)(23) = f_4$,

$f_3 f_3 = (13)(24)(13)(24) = (13)(13)(24)(24) = (I)(I) = I = f_1$,

$f_3 f_4 = (13)(24)(14)(23) = (12)(34) = f_2$,

$f_4 f_2 = (14)(23)(12)(34) = (13)(24) = f_3$,

$f_4 f_3 = (14)(23)(13)(24) = (12)(34) = f_2$

and $f_4 f_4 = (14)(23)(14)(23) = (14)(14)(23)(23) = (I)(I) = I = f_1$.

Making all these calculations the composition table for G is as given below :

Product of permutations	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Now we make the following observations :

(i) All the entries in the composition table are elements of the given set G. Therefore G is closed for product of permutations.

(ii) We know that the product of permutations is an associative operation.

(iii) f_1 is the identity element.

(iv) Each element of G possesses inverse.
In fact $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$.

(v) Since the corresponding rows and columns in the composition table for G are identical, therefore the operation of product of permutations is commutative on the given set G.
Hence the given set G is a finite abelian group of order 4 with respect to the permutation multiplication.

Problem 12: *Show that the $n!$ permutations of n objects form a group with respect to permutation multiplication. Verify this theorem by taking the set of all permutations of the elements* 1, 2, 3. **(Gorakhpur 2005; Kumaun 12)**

Solution: First give the proof of the theorem of article 2. Then give the solution given in solved example 4.

Problem 13: *Show that if a set S has more than two elements, then the symmetric group S_n is not abelian.*

Solution: Let $S = \{a_1, a_2, \ldots, a_n\}$, where $n > 2$. We have to show that the symmetric group S_n is not abelian. For this we have to produce two permutations on the set S whose product is not commutative.

Consider the permutations

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_{n-1} & a_n \\ a_2 & a_3 & a_4 \ldots a_n & a_1 \end{pmatrix}$$

and $$g = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \ldots a_n \\ a_2 & a_1 & a_3 & a_4 \ldots a_n \end{pmatrix}$$ on the set S.

We have $$fg = \begin{pmatrix} a_1 & a_2 \ldots a_{n-1} & a_n \\ a_1 & a_3 \ldots a_n & a_2 \end{pmatrix}$$

and $$gf = \begin{pmatrix} a_1 & a_2 & a_3 \ldots a_n \\ a_3 & a_2 & a_4 \ldots a_n \end{pmatrix}.$$

We see that under the permutation fg the image of a_1 is a_1 while under the permutation gf the image of a_1 is a_3. Therefore we have $fg \neq gf$. Thus if $n > 2$, then the operation of the product of permutations on the set S_n is not commutative and consequently the group S_n is not abelian.

Problem 14: *G is a finite group and a is a fixed element of G. Show that the mapping $f_a : G \to G$ defined by $f_a(x) = ax \; \forall \; x \in G$ is a permutation on G, i.e., is one-to-one mapping of G onto G.*

Solution: Let G be a finite group. If $a \in G$, then for every x in G the product ax is also an element of G and is unique. Therefore $f_a(x) = ax \; \forall \; x \in G$ defines a mapping from G to G. In order to show that the mapping f_a is a permutation on G, we have to show that f_a is one-to-one and also onto.

The mapping f_a is **one-to-one** because if $x, y \in G$, then

$$f_a(x) = f_a(y) \quad \Rightarrow \quad ax = ay$$

$\Rightarrow$ $x = y$, by left cancellation law in the group G.

The mapping f_a is also onto G because if x is any element of G, then $\exists$ an element $a^{-1}x$ in G such that

$$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = ex = x.$$

Thus f_a is a one-to-one mapping of G onto G. Hence f_a is a permutation on G.

Hints to Objective Type Questions

Multiple Choice Questions

1. We have $f\,g = (23)\,(123) = (12)\,(3) = (12)$.

2. See article 15.

The total number of all even permutations of degree n is $\frac{n!}{2}$.

Thus, the order of the group A_n *i.e.*, the number of distinct elements in the group A_n is $\frac{n!}{2}$.

3. We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 4 & 3 & 1 & 7 \end{pmatrix}$

$= (1\quad 6)\,(2\quad 5\quad 3)\,(4)\,(7) = (1\quad 6)\,(2\quad 5\quad 3)$

$= (1\quad 6)\,(2\quad 5)\,(2\quad 3)$.

4. See article 13, Corollary 1.

5. See article 13, Theorem.

6. See article 6, Note 3.

7. We have $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

$\therefore \quad AB = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

8. We have $A = \begin{pmatrix} 3 & 4 & 9 \\ 2 & 7 & 8 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 8 & 7 \\ 11 & 12 & 13 \end{pmatrix}$.

$\therefore \quad AB = \begin{pmatrix} 3 & 4 & 9 \\ 2 & 7 & 8 \end{pmatrix}\begin{pmatrix} 2 & 8 & 7 \\ 11 & 12 & 13 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 9 \\ 11 & 13 & 12 \end{pmatrix}$.

9. We have $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

$\therefore \quad AB = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

10. See article 15.

11. See article 13, Corollary 1 and article 14.

12. See Corollary 2 of article 13.

13. Number of elements of order r in the symmetric group

$$S_n = \frac{{}^nP_r}{r} = \frac{5!}{5} = 4 \times 3 \times 2 \times 1 = 24.$$

14. See article 6, Note 3.

15. See Problem 4(ii) of Comprehensive Problems 1.

Fill in the Blank(s)

1. See article 1. Definition of a permutation.

2. See article 6. The number of distinct elements in the group P_n is n !.

So, the order of the group P_n is n !.

3. See Corollary 2 of article 13.

4. See Corollary 4 of article 13.

5. We have $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

$$\therefore \quad fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

6. $fg = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 \end{pmatrix}$.

7. We have $fg = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix}\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$.

True or False

1. The group P_3 is non-abelian. See Example 4.

2. See article 8, the definition of transposition.

3. See article 10.

4. See article 12, Theorem 1.

5. See article 12, Theorem 3.

6. See article 13, Corollary 1.

❍❍❍

Chapter-5

Homomorphism and Isomorphism of Groups

Comprehensive Problems 1

Problem 1: *Show that the mapping* $f : G \to G'$ *defined by* $f(x) = 2x \ \forall \ x \in G$ *is an isomorphism of* G *into* G' *where* G *is the additive group of integers and* G' *is the additive group of even integers including zero.*

Solution: If $x \in G$, then obviously $2x \in G'$.

f is one-to-one: Let $x_1, x_2 \in G$. Then $f(x_1) = f(x_2)$

$\Rightarrow \quad 2x_1 = 2x_2$ [By def. of f]

$\Rightarrow \quad x_1 = x_2$ [$\because \ 2 \neq 0$]

Therefore f is one-to-one.

f is onto: Suppose y is any element of G'.Then obviously $\frac{y}{2} \in G$.

Also $f\left(\frac{y}{2}\right) = 2\left(\frac{y}{2}\right) = y$.Thus $y \in G' \ \Rightarrow$ that these exist $\frac{y}{2} \in G$ such that $f\left(\frac{y}{2}\right) = y$.

Therefore each element of G' is the f –image of some element of G. Hence f is onto.

Again if x_1 and x_2 are any two elements of G ,then

$f(x_1 + x_2) = 2(x_1 + x_2)$ [By def. of f]

$= (2x_1 + 2x_2)$ [By distributive law for integers]

$= f(x_1) + f(x_2)$ [By def. of f]

Thus f preserves compositions in G and G'.Therefore f is an isomorphic mapping of G onto G'. Hence G is isomorphic to G'.

Problem 2: *Show that the additive group* G *of all integers is isomorphic to the multiplicative group*

$$G' = \{..., 3^{-3}, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, 3^3, ...\}.$$

Solution: If $x \in G$, then obviously $3^x \in G'$. Let $f : G \Rightarrow G'$ be defined by $f(x) = 3^x \ \forall \ x \in G$.

f is one-to-one. Let $x, y \in G$. Then $f(x) = f(y) \Rightarrow 3^x = 3^y \Rightarrow x = y$.

$\therefore \quad f$ is one-to-one.

f is onto: Let y be any element of G'. Then $y = 3^x$ where x is some integer. Now $x \in G$ is such that $f(x) = 3^x = y$. Therefore each element of G' is the f-image of some element of G. Hence f is onto.

f is composition-preserving: Let x, y be any two elements of G. Then

$$f(x + y) = 3^{x+y} = 3^x 3^y = f(x) f(y).$$

Thus f preserves compositions in G and G'. Therefore f is an isomorphism of G onto G'. Hence G is isomorphic to G'.

Problem 3: *Show that the real matrices of the type* $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, *where* $a \neq 0$ *form a multiplicative group which is isomorphic to the group of non-zero real numbers under multiplication.*

Solution: Let G denote the set of all real matrices of the type $\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, where $a \neq 0$. To show that G is a group for multiplication of matrices.

Closure property: Let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}$ be any two members of G where $a, b \in \mathbf{R}$ and $a \neq 0, b \neq 0$. Here $\mathbf{R}$ denotes the set of real numbers.

We have $AB = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}$ which is definitely a member of G because $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$ and so $ab \in \mathbf{R}$ and $ab \neq 0$.

Associativity: We know that matrix multiplication is associative.

Existence of identity: If we take $a = 1$, then we observe that the unit matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ and is such that $IA = A = AI, \ \forall\, A \in G$.

Existence of inverse: Let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ be any member of G, where $a \in \mathbf{R}$ and $a \neq 0$.

We have $\det A = a \neq 0$ and so the matrix A is non-singular and hence is invertible.

We have $$A^{-1} = \frac{1}{|A|}\text{adj. } A = \frac{1}{a}\begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1/a & 0 \\ 0 & 1 \end{bmatrix}$$

which is surely a member of G because $1/a \in \mathbf{R}$ and $1/a \neq 0$. Thus each member of G has its multiplicative inverse in G.

Hence G is a group for multiplication of matrices.

Now let G' denote the multiplicative group of all non-zero real numbers. Then to show that

$$G \cong G'.$$

Let $f : G \to G'$ be defined by $f\left(\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}\right) = a, \ \forall \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in G$.

***f* is one-to-one:** Let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}$ be any two members of G. Then

$$f(A) = f(B) \Rightarrow a = b \ \Rightarrow \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow A = B$$

$\therefore$ f is one-to-one.

f is onto: Let a be any element of G'. Then there exists $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in G$ such that $f(A) = a$.

Therefore each element of G' is the f-image of some member of G. Hence f is onto.

f is composition-preserving: Let $A = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} b & 0 \\ 0 & 1 \end{bmatrix}$ be any two members of G. Then

$$f(AB) = f\left(\begin{bmatrix} ab & 0 \\ 0 & 1 \end{bmatrix}\right) = ab = f(A)\, f(B).$$

Thus f preserves compositions in G and G'.

Therefore f is an isomorphism of G onto G'. Hence G is isomorphic to G'.

Problem 4: *Show that the multiplicative group of all matrices* $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, *where a and b are real numbers (not both equal to zero), is isomorphic to the group of non-zero complex numbers for multiplication.*

Solution: Let G denote the multiplicative group of all matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where a and b are real numbers such that at least one of them is not equal to zero so that $a + ib$ is a non-zero complex number. If G' denotes the multiplicative group of non-zero complex numbers, then to show that $G \cong G'$.

Let $f : G \Rightarrow G'$ be defined by

$$f\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a + ib, \ \forall \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G.$$

f is one-to-one: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be any two members of G.

Then $f(A) = f(B) \Rightarrow a + ib = c + id \Rightarrow a = c,\ b = d$

$$\Rightarrow \quad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \Rightarrow A = B.$$

$\therefore$ f is one-to-one.

f is onto: Let $a + ib$ be any member of G'. Then there exists $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in G$ such that $f(A) = a + ib$. Therefore each member of G' is the f-image of some member of G. Hence f is onto.

f is composition-preserving: Let $A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $B = \begin{bmatrix} c & d \\ -d & c \end{bmatrix}$ be any two members of G. Then

$$AB = \begin{bmatrix} ac - bd & ad + bc \\ -bc - ad & ac - bd \end{bmatrix}.$$

We have $f(AB) = (ac - bd) + i(ad + bc) = (a + ib)(c + id) = f(A)\, f(B).$

Thus f preserves compositions in G and G'.
Therefore f is an isomorphism of G onto G'.
Hence G is isomorphic to G'.

Problem 5: *Prove that the additive group G of complex numbers $a + ib$ (a, b integers) is isomorphic to the multiplicative group G' of rationals of the form $2^a 3^b$ (a, b integers).*

Solution: Let $f : G \to G'$ be defined by $f(a + ib) = 2^a 3^b, \forall\ a + ib \in G$.

f is one-to-one: Let $a + ib$ and $c + id$ be any two members of G. Then a, b, c and d are all integers. We have $f(a + ib) = f(c + id) \Rightarrow 2^a 3^b = 2^c 3^d \Rightarrow 2^{a-c} = 3^{d-b}$

$\Rightarrow$ $a - c = 0$ and $d - b = 0$ because otherwise we cannot have $2^{a-c} = 3^{d-b}$

$\Rightarrow$ $a = c$ and $d = b \Rightarrow a + ib = c + id$.

$\therefore$ f is one-to-one.

f is onto: Let $2^a 3^b$ be any member of G'. Then there exists $a + ib \in G$ such that $f(a + ib) = 2^a 3^b$.

Therefore f is onto.

f is composition preserving: Let $a + ib$ and $c + id$ be any two members of G. Then

$$f[(a + ib) + (c + id)] = f[(a + c) + i(b + d)]$$
$$= 2^{a+c} 3^{b+d} = (2^a 3^b)(2^c 3^d) = f(a + ib)\, f(c + id).$$

Thus f preserves compositions in G and G'.
Therefore f is an isomorphism of G onto G'. Hence G is isomorphic to G'.

Comprehensive Problems 2

Problem 1: *Show that the multiplicative group $G = (\{1, -1\}, \bullet)$ is isomorphic to the permutation group $G' = (\{I, (ab)\}, o)$.*

Solution: Here the identity of the group G is 1 and that of the group G' is the identity permutation I.
Consider the mapping $f : G \to G'$ defined by

$$f(1) = I \quad \text{and} \quad f(-1) = (ab).$$

Obviously the mapping f is one-one and onto. Furthermore

$$f(1.1) = f(1) = I = I\ o\ I = f(1)\ o\ f(1),$$
$$f[1.(-1)] = f(-1) = (ab) = I\ o\ (ab) = f(1)\ o\ f(-1),$$
$$f[(-1).1] = f(-1) = (ab) = (ab)\ o\ I = f(-1)\ o\ f(1),$$
$$f[(-1).(-1)] = f(1) = I = (ab)\ o\ (ab) = f(-1)\ o\ f(-1).$$

Thus $f(x.y) = f(x)\ o\ f(y)\ \forall\ x, y \in G$ and so the mapping f preserves compositions in G and G'.
Therefore the mapping f is an isomorphism of G onto G'. Hence the group G is isomorphic to the group G'.

Problem 2: *Show that the multiplicative group $G = \{1, -1\}$ is isomorphic to the group $G' = (\{f_1, f_2\}, o)$, where $f_1 : \mathbf{R} \to \mathbf{R} : f_1(x) = x$, $f_2 : \mathbf{R} \to \mathbf{R} : f_2(x) = 1 - x$.*

Solution: Here the identity of the group G is 1.

In the case of the group G' the mapping f_1 is the identity mapping of the set **R** because $f_1(x) = x, \forall\ x \in \mathbf{R}$. Let x be any element of **R.** Then

$$(f_1 \circ f_1)(x) = f_1[f_1(x)] = f_1(x) \Rightarrow f_1 \circ f_1 = f_1,$$
$$(f_1 \circ f_2)(x) = f_1[f_2(x)] = f_1(1-x) = 1 - x = f_2(x)$$
$$\Rightarrow f_1 \circ f_2 = f_2,$$
$$(f_2 \circ f_1)(x) = f_2[f_1(x)] = f_2(x) \Rightarrow f_2 \circ f_1 = f_2,$$
$$(f_2 \circ f_2)(x) = f_2[f_2(x)] = f_2(1-x) = 1 - (1-x) = x = f_1(x)$$
$$\Rightarrow f_2 \circ f_2 = f_1.$$

We observe that the identity of the group G' is f_1.

Consider the mapping $\phi : G \to G'$ defined by

$$\phi(1) = f_1 \text{ and } \phi(-1) = f_2.$$

Obviously the mapping ϕ is one-one and onto. Furthermore

$$\phi(1.1) = \phi(1) = f_1 = f_1 \circ f_1 = \phi(1) \circ \phi(1),$$
$$\phi[1.(-1)] = \phi(-1) = f_2 = f_1 \circ f_2 = \phi(1) \circ \phi(-1),$$
$$\phi[(-1).1] = \phi(-1) = f_2 = f_2 \circ f_1 = \phi(-1) \circ \phi(1),$$
$$\phi[(-1).(-1)] = \phi(1) = f_1 = f_2 \circ f_2 = \phi(-1) \circ \phi(-1).$$

Thus, $\phi(x.y) = \phi(x) \circ \phi(y), \quad \forall\ x, y \in G$ and so the mapping ϕ preserves compositions in G and G'.

Therefore the mapping ϕ is an isomorphism of G onto G'. Hence the group G is isomorphic to the group G'.

Problem 3: *Show that the group* $G = (\{0, 1, 2, 3\}, +_4)$ *is isomorphic to the group* $G' = (\{1, 2, 3, 4\}, \times_5)$.

Solution: Here 0 is the identity of G and 1 is the identity of G'. Therefore if $f : G \to G'$ is to be an isomorphism of G onto G', we must have $f(0) = 1$.

In the group G the orders of 1, 2, 3 are 4, 2 and 4 respectively. In the group G' the orders of 2, 3, 4 are 4, 4 and 2 respectively. Therefore we must take $f(2) = 4$. Further let us take $f(1) = 2$, $f(3) = 3$.

The mapping f is obviously one-one onto. To show that f preserves compositions in G and G', we should proceed as in problem 1.

Problem 4: *Show that the multiplicative group* $G = \{1, \omega, \omega^2\}$ *is isomorphic to the group* G' *of residue classes* (*mod* 3) *under addition of residue classes.*

Solution: The group G' consists of the residue classes $\overline{0}$, $\overline{1}$ and $\overline{2}$.

Here the identity of the group G is 1 and that of the group G' is the residue class $\overline{0}$. If f is to be an isomorphism of G onto G', we must have $f(1) = \overline{0}$, *i.e.*, identity must go to identity.

In the group G each of the elements ω and ω^2 is of order 3 while in the group G' each of the elements $\overline{1}$ and $\overline{2}$ is of order 3.

Consider the mapping $f : G \to G'$ defined as follows :

$$f(1) = \overline{0},\ f(\omega) = \overline{1},\ f(\omega^2) = \overline{2}.$$

Obviously the mapping f is one-one and onto. To show that f preserves compositions in G and G' we proceed as follows :

Let us write $A_1 = 1, A_2 = \omega, A_3 = \omega^2$.

We shall denote the corresponding f-images in G' by writing B in place of A. So let us write

$$B_1 = f(A_1) = f(1) = \overline{0}, B_2 = f(A_2) = f(\omega) = \overline{1},$$
$$B_3 = f(A_3) = f(\omega^2) = \overline{2}.$$

Now we shall form the composition tables for the two groups G and G'.

Composition table for G

$\cdot$		A_1	A_2	A_3
		1	ω	ω^2
A_1	1	A_1	A_2	A_3
A_2	ω	A_2	A_3	A_1
A_3	ω^2	A_3	A_1	A_2

Composition table for G'

$+$		B_1	B_2	B_3
		$\overline{0}$	$\overline{1}$	$\overline{2}$
B_1	$\overline{0}$	B_1	B_2	B_3
B_2	$\overline{1}$	B_2	B_3	B_1
B_3	$\overline{2}$	B_3	B_1	B_2

Note that $B_2 + B_2 = \overline{1} + \overline{1} = \overline{2} = B_3$, $B_2 + B_3 = \overline{1} + \overline{2} = \overline{3} = \overline{0} = B_1$,

$B_3 + B_2 = \overline{2} + \overline{1} = \overline{3} = 0 = B_1, B_3 + B_3 = \overline{2} + \overline{2} = \overline{4} = \overline{1} = B_2$, etc.

We see that the composition tables for G and G' are identical. Therefore the mapping f must preserve compositions in G and G' as shown below:

Let $A_i , A_j \in G$ and let $A_i . A_j = A_k$. We have

$f(A_i) = B_i , f(A_j) = B_j$ and $B_i + B_j = B_k$.

Now $f(A_i . A_j) = f(A_k) = B_k = B_i + B_j = f(A_i) + f(A_j)$.

Thus $f(A_i . A_j) = f(A_i) + f(A_j),\ \forall\ A_i , A_j \in G$.

$\therefore$ The mapping f preserves compositions in G and G'.

Thus f is an isomorphism of G onto G'. Hence the group G is isomorphic to the group G'.

Note: The mapping $\phi : G \to G'$ defined by

$$\phi(1) = \overline{0},\ \phi(\omega) = \overline{2},\ \phi(\omega^2) = \overline{1}$$

is also an isomorphism of G and G' as can be easily seen.

Problem 5: *Show that the multiplicative group $G = \{1, \omega, \omega^2\}$ is isomorphic to the permutation group $G' = \{I, (abc), (acb)\}$ on three symbols a, b, c.*

(Kanpur 2010; Kumaun 09, 12)

Solution: Proceed as in problem 4. Take the mapping $f : G \to G'$ defined as

$$f(1) = I,\ f(\omega) = (abc),\ f(\omega^2) = (acb).$$

Problem 6: *Show that the multiplicative group* $G = \{1, -1, i, -i\}$ *is isomorphic to the group* $G' = \{0, 1, 2, 3\}$ *with addition modulo* 4 *as composition.*

Solution: We note that the identity of the group G is 1 and that of the group G' is 0. Therefore if f is to be an isomorphism of G onto G', then we must have $f(1) = 0$, *i.e.*, identity must go to identity.

In the group G the orders of -1, i and $-i$ are 2, 4 and 4 respectively. While in the group G' the orders of 1, 2 and 3 are 4, 2 and 4 respectively. In an isomorphic mapping only elements of equal order can be mapped on each other. Therefore we must have $f(-1) = 2$. Now the f-image of i can be taken either 1 or 3. Let us take $f(i) = 1$ and $f(-i) = 3$.

Thus the mapping $f : G \to G'$ is defined as follows:

$$f(1) = 0, \quad f(-1) = 2, \quad f(i) = 1, \quad f(-i) = 3.$$

Obviously the mapping f is one-one and onto. To show that f preserves compositions in G and G' we proceed as follows:

Let us write $A_1 = 1$, $A_2 = -1$, $A_3 = i$ and $A_4 = -i$. We shall denote the corresponding f-images in G' by writing B in place of A. So let us write

$$B_1 = f(A_1) = f(1) = 0,$$
$$B_2 = f(A_2) = f(-1) = 2,$$
$$B_3 = f(A_3) = f(i) = 1$$

and
$$B_4 = f(A_4) = f(-i) = 3.$$

Now we shall form the composition tables for the two groups G and G' :

Composition table for G

		A_1 1	A_2 -1	A_3 i	A_4 $-i$
A_1	1	A_1	A_2	A_3	A_4
A_2	-1	A_2	A_1	A_4	A_3
A_3	i	A_3	A_4	A_2	A_1
A_4	$-i$	A_4	A_3	A_1	A_2

Composition table for G'

$+_4$		B_1 0	B_2 2	B_3 1	B_4 3
B_1	0	B_1	B_2	B_3	B_4
B_2	2	B_2	B_1	B_4	B_3
B_3	1	B_3	B_4	B_2	B_1
B_4	3	B_4	B_3	B_1	B_2

We see that the composition tables for G and G' are identical *i.e.*, if we replace A_1, A_2, A_3, A_4 by B_1, B_2, B_3, B_4 in the composition table for G, we reproduce the complete composition table for G'. Therefore the mapping f must preserve compositions in G and G' as shown below:

Let $A_i, A_j \Rightarrow G$ and let $A_i \cdot A_j = A_k$. We have

$$f(A_i) = B_i \text{ and } f(A_j) = B_j \text{ and } B_i +_4 B_j = B_k.$$

Now
$$f(A_i \cdot A_j) = f(A_k) = B_k = B_i +_4 B_j = f(A_i) +_4 f(A_j).$$

Thus
$$f(A_i \cdot A_j) = f(A_i) +_4 f(A_j), \ \forall A_i, A_j \in G.$$

$\therefore$ The mapping f preserves compositions in G and G'.

Thus f is an isomorphism of G onto G'. Hence the group G is isomorphic to the group G'.

Note: The mapping $\phi : G \to G'$ defined by $\phi(1) = 0, \phi(-1) = 2, \phi(i) = 3, \phi(-i) = 1$ is also an isomorphism of G onto G' as can be easily seen. Also it is obvious that in this case we can have only two isomorphisms of G onto G'.

Comprehensive Problems 3

Problem 1: *What do you understand by the statement :*

"When two groups are isomorphic, then in some sense they are equal".

Solution: If a group G is isomorphic to a group G', we say that the groups G and G' are **abstractly identical**. From the point of view of abstract algebra we shall regard them as one group and not as two different groups. The two isomorphic groups may have different elements and different binary operations. For a common man the two groups may present distinct appearance but from the point of view of algebraic structure we shall say that the two groups are equal.

Problem 2: *If f is an isomorphism of a group G onto a group G', show that f^{-1} is an isomorphism of G' onto G.*

Solution: Let f be an isomorphism of a group G onto a group G', the operations on both the groups denoted multiplicatively. Then the mapping f is one-one onto and preserves compositions in G and G'. Since f is one-one onto, therefore it is inversible, *i.e.*, f^{-1} exists. Also we know that the inverse mapping f^{-1} is also one-one onto.

Now we shall show that $f^{-1} : G' \to G$ is also composition preserving. Let a', b' be any elements of G'. Then there exist elements $a, b \in G$ such that

$$f^{-1}(a') = a, \; f^{-1}(b') = b \qquad \ldots(1)$$

and $$f(a) = a', \; f(b) = b'. \qquad \ldots(2)$$

Now $$f^{-1}(a'b') = f^{-1}[f(a) f(b)] \qquad [\text{From (2)}]$$

$$= f^{-1}[f(ab)], \text{ since } f(ab) = f(a) f(b)$$

$$= ab \qquad [\text{By def. of inverse mapping } f^{-1}]$$

$$= f^{-1}(a') f^{-1}(b'). \qquad [\text{From (1)}]$$

$\therefore$ The mapping f^{-1} preserves compositions in G' and G.

Hence f^{-1} is an isomorphism of G' onto G.

Problem 3: *Show that the product (or composite) of two isomorphisms is also an isomorphism.*

Solution: Let f be an isomorphism of a group G onto a group G' and g be an isomorphism of the group G' onto a group G'', the operations on all the three groups G, G' and G'' denoted multiplicatively.

We know that the composite mapping $g \circ f : G \to G''$ is defined by

$$(g \circ f)(x) = g[f(x)] \; \forall \, x \in G.$$

To show that the mapping $g \circ f$ is also an isomorphism of G onto G''.

Since the mappings f and g are one-one and onto, their composite mapping $g \circ f$ is also one-one and onto.

Now to show that the mapping $g \circ f$ preserves compositions in G and G''. Let x, y be any elements of G. Then

$$(g \circ f)(x) = g[f(xy)] \quad \text{[By def. of composite mapping } g \circ f \text{]}$$
$$= g[f(x) f(y)] \quad [\because f \text{ is composition preserving}]$$
$$= g[f(x)]\, g[f(y)] \quad [\because g \text{ is also composition preserving}]$$
$$= [(g \circ f)(x)][(g \circ f)(y)].$$

Thus the mapping $g \circ f$ preserves compositions in G and G''.

Hence $g \circ f$ is an isomorphism of G onto G''.

Problem 4: *Let G be any group and a be any fixed element in G. Define a mapping $f : G \to G$ by the formula $f(x) = axa^{-1}, \forall x \in G$.*

Prove that f is an isomorphism of G onto itself.

Solution: The mapping f is **one-to-one.** Let x, y be any two elements of G. Then

$f(x) = f(y) \Rightarrow axa^{-1} = aya^{-1} \Rightarrow x = y$, by left and right cancellation laws in G.

$\therefore$ The mapping f is one-one.

The mapping f is also **onto** G. If y is any element of G, then $a^{-1} ya \in G$ and we have

$$f(a^{-1} ya) = a(a^{-1} ya)\, a^{-1} = (aa^{-1})\, y\, (aa^{-1}) = e\, y\, e = y.$$

$\therefore$ The mapping f is onto G.

Finally, if $x, y \in G$ then $f(xy) = a(xy)\, a^{-1} = (axa^{-1})(aya^{-1}) = f(x)\, f(y)$.

Hence f is an isomorphism of G onto itself.

Problem 5: *Prove that the order of an element of a group is unaltered by an isomorphism.*

Solution: For complete solution of this question refer theorem 2 of article 4.

Problem 6: *Show that the mapping $x \to x^{-1}$ of G onto G is an isomorphism if and only if G is abelian, x being any element of the group G.*

Solution: Let $f : G \to G$ be such that $f(x) = x^{-1}\ \forall x \in G$. The mapping f is one-one because

$$f(x) = f(y) \Rightarrow x^{-1} = y^{-1} \Rightarrow (x^{-1})^{-1} = (y^{-1})^{-1} \Rightarrow x = y.$$

Also if $x \in G$, then $x^{-1} \in G$ and we have $f(x^{-1}) = (x^{-1})^{-1} = x$.

$\therefore$ f is onto.

Now suppose G is abelian. Let a, b be any two elements of G.

Then
$$f(ab) = (ab)^{-1} \quad \text{[By def. of } f \text{]}$$
$$= b^{-1} a^{-1} = a^{-1} b^{-1} \quad [\because\ G \text{ is abelian}]$$
$$= f(a)\, f(b) \quad \text{[By def. of } f \text{]}$$

$\therefore$ f is an isomorphism of G onto G.

Conversely suppose that f is an isomorphism of G onto G. Let $a, b \in G$.

We have $f(ab) = (ab)^{-1}$ [By def. of f]

$= b^{-1} a^{-1} = f(b) f(a)$ [By def. of f]

$= f(ba)$ [$\because$ f is an isomorphism]

Since f is one-one, therefore

$f(ab) = f(ba) \Rightarrow ab = ba \Rightarrow$ the group G is abelian.

Hints to Objective Type Questions

Multiple Choice Questions

1. See article 2.
2. See article 1.
3. See article 1.
4. See article 1.

Fill in the Blank(s)

1. See Theorem of article 5.
2. See article 3, Note 4.
3. See article 2.

True or False

1. See article 4, Theorem 2.
2. See article 4, Theorem 1 (i).
3. See article 4, Theorem 1 (ii).

○○○

Chapter-6

Subgroups, Cosets and Lagrange's Theorem

Comprehensive Problems 1

Problem 1: (*i*) *Define a subgroup. Give examples.*

(*ii*) *What is the difference between a complex and a subgroup of a group?*

Solution: For a complete solution of this question read article 1.

Problem 2: *Define alternating group. Show that the alternating group A_n is a subgroup of the symmetric group S_n of the permutations over n objects. Write down all the proper subgroups of S_3 .*

Solution: Let $S = \{a_1, a_2, ..., a_n\}$ be a set consisting of n objects. The set S_n of all $n!$ permutations on the set S is a group for composite of permutations. This group S_n is called the **symmetric group of permutations over *n* objects.** The order of this group is $n!$.

Alternating group: Out of the $n!$ permutations over n objects half are even permutations and half are odd permutations. If A_n is the set of all even permutations over n objects, then A_n is also a group for composite of permutations. This group A_n is called **'Alternating group'.**

We have $A_n \subset S_n$ where S_n is a finite group. We know that the product of two even permutations is also an even permutation. Therefore $f \in A_n$, $g \in A_n \Rightarrow f\,g \in A_n$. Thus A_n is a non-empty finite subset of S_n and is closed for the operation of the group S_n *i.e.*, for the operation of composite of two permutations. Hence A_n is a subgroup of S_n .

The symmetric group S_3 of 3 ! permutations on three objects *a, b, c* has the following six members :

$$S_3 = \{I \text{ (}i.e.\text{, identity permutation)}, (ab), (bc), (ca), (abc), (acb)\}.$$

There are four proper subgroups of S_3 and they are as given below :

$$\{I, (ab)\}, \{I, (bc)\}, \{I, (ca)\}, \{I, (abc), (acb)\}.$$

Problem 3: *Verify the following statements for being true or false. In case a statement is false, write the corresponding correct statement.*

(*i*) *A non-empty subset H of a group G, which is closed under the binary composition in G, is a subgroup of G.*

(*ii*) *If G is a group and H is a non-empty subset of G, then H will be a subgroup of G if $H^2 = H$.*

Solution: (i) The given statement is false. For example let G be the additive group of all integers $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ and H be the subset of G consisting of all positive integers *i.e.*, $H = \{1, 2, 3, 4, ...\}$. Obviously H is closed with respect to addition *i.e.*, the composition in G. But H is not a subgroup of G since the identity $0 \approx H$.

The corresponding correct statement is 'A non-empty **finite** subset H of a group G, which is closed under the binary composition in G, is a subgroup of G'.

(ii) The given statement is false. For example let

$$G = \{..., 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, ...\}$$

be the multiplicative group consisting of integral powers of 2. Let $H = \{1, 2, 2^2, 2^3, ...\}$. Then $H \subseteq G$ and $HH = H$, *i.e.*, $H^2 = H$. But H is not a subgroup of G since the inverse of 2 *i.e.*, 2^{-1} does not belong to H.

The corresponding correct statement is 'If G is a group and H is a non-empty **finite** subset of G, then H will be a subgroup of G if $H^2 = H$'.

Problem 4: *If G is a group, the centre of G, Z is defined by*

$$Z = \{z \in G : zx = xz \ \forall x \in G\}.$$

Prove that Z is a subgroup of G.

Or

Show that the elements in a group G which commute with every element of G form a subgroup of G.

Solution: We have $Z = \{z \in G : zx = xz \ \forall x \in G\}$ *i.e.*, Z consists of those elements of G which commute with every element of G.

To show that Z is a subgroup of G.

Since $e \in G$ is such that $ex = xe \ \forall x \in G$, therefore at least $e \in Z$ and so $Z \neq \varnothing$.

Now let $z_1, z_2 \in Z$. Then $z_1 x = x z_1$ and $z_2 x = x z_2$ for all $x \in G$.

First we shall show that $z_2^{-1} \in Z$.

We have $z_2 x = x z_2 \ \forall x \in G$

$\Rightarrow$ $z_2^{-1} (z_2 x) z_2^{-1} = z_2^{-1} (x z_2) z_2^{-1}$

$\Rightarrow$ $x z_2^{-1} = z_2^{-1} x \ \forall x \in G \ \Rightarrow \ z_2^{-1} \in Z$.

Now for all $x \in G$, we have

$$(z_1 z_2^{-1}) x = z_1 (z_2^{-1} x) = z_1 (x z_2^{-1}) = (z_1 x) z_2^{-1}$$

$$= (x z_1) z_2^{-1} = x (z_1 z_2^{-1}).$$

$\therefore$ By def. of Z, $z_1 z_2^{-1} \in Z$.

Thus $z_1, z_2 \in Z \Rightarrow z_1 z_2^{-1} \in Z$. Hence Z is a subgroup of G.

Problem 5: *If $a \in G$, we define* $N(a) = \{x \in G : ax = xa\}$.

Show that $N(a)$ is a subgroup of G.

Solution: We have $N(a) = \{x \in G : ax = xa\}$.

Since $e \in G$ is such that $ea = ae$, therefore at least $e \in N(a)$ and so $N(a) \neq \varnothing$.

Now let $x_1, x_2 \in N(a)$. Then $ax_1 = x_1 a, ax_2 = x_2 a$.

First we show that $x_2^{-1} \in N(a)$.

We have $ax_2 = x_2 a \ \Rightarrow \ x_2^{-1} (ax_2) x_2^{-1} = x_2^{-1} (x_2 a) x_2^{-1}$

$\Rightarrow$ $x_2^{-1} a = a x_2^{-1} \ \Rightarrow \ x_2^{-1} \in N(a)$.

Now we shall show that $x_1 x_2^{-1} \in N(a)$.

We have $a(x_1 x_2^{-1}) = (ax_1) x_2^{-1} = (x_1 a) x_2^{-1}$

$= x_1 (ax_2^{-1}) = x_1 (x_2^{-1} a) = (x_1 x_2^{-1}) a.$

$\therefore$ By def. of $N(a)$, $x_1 x_2^{-1} \in N(a)$.

Thus $x_1, x_2 \in N(a) \Rightarrow x_1 x_2^{-1} \in N(a)$.

Hence $N(a)$ is a subgroup of G.

Problem 6: *Show that the integral multiples of* 5 *form a subgroup of the additive group of integers.*

Solution: Let $(\mathbf{I}, +)$ be the additive group of integers where

$\mathbf{I} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.

Let H consist of the integral multiples of 5 *i.e.*, let $H = \{5x : x \in \mathbf{I}\}$.

Then H is a non-empty subset of $\mathbf{I}$. We have to show that H is a subgroup of the group $(\mathbf{I}, +)$.

Let $a = 5r$ and $b = 5s$ be any two elements of H where r and s are some integers.

We have $a - b = 5r - 5s = 5(r - s) \in H$ because $r - s$ is also some integer. Thus $a \in H$, $b \in H \Rightarrow a - b \in H$. Hence H is a subgroup of the group $(\mathbf{I}, +)$.

Problem 7: *Let A and B be subgroups of a group G and let AB be the subset of G consisting of all elements of the form ab, where a is in A and b is in B. Then*

(*i*) *Show by considering the subgroups of the group of permutations of three elements, or otherwise, that AB need not be a subgroup of G.*

(*ii*) *Show that AB is a subgroup of G if and only if AB = BA.*

Solution: (i) Let P_3 be the symmetric group of permutations on three objects a, b, c.

Then $P_3 = \{I, (ab), (bc), (ca), (abc), (acb)\}$, where I denotes the identity permutation on the set $\{a, b, c\}$.

Consider the subgroups $A = \{I, (ab)\}$ and $B = \{I, (bc)\}$ of P_3.

We have $AB = \{(I)(I), I(bc), (ab)I, (ab)(bc)\} = \{I, (bc), (ab), (acb)\}$.

The inverse of the permutation (acb) is the permutation (bca) *i.e.*, (abc) which is not a member of AB. But in a subgroup the inverse of each element must be present in it. Hence AB is not a subgroup of P_3.

(ii) For complete solution of this part of the question see theorem 1 of article 4.

Problem 8: *Show that the* 24 *permutations on* 4 *symbols form a group with respect to permutation multiplication. Write down three proper subgroups of this group.*

Solution: Let P_4 denote the set of 4! *i.e.*, 24 permutations on four symbols a_1, a_2, a_3, a_4. To prove that P_4 is a group for composite of permutations proceed as in the theorem of article 4 of Chapter Permutation Group by taking $n = 4$.

Let I denote the identity permutation on the set $\{a_1, a_2, a_3, a_4\}$. Three proper subgroups of the group P_4 are :

$\{I, (a_1\ a_2)\}, \{I, (a_2\ a_3)\}, \{I, (a_3\ a_4)\}$.

Problem 9: *Let G be a group, H a subgroup of G. Let for $x \in G$, $xHx^{-1} = \{xhx^{-1} : h \in H\}$. Prove that xHx^{-1} is a subgroup of G.*

Solution: We have $xHx^{-1} = \{xhx^{-1} : h \in H\}$, where x is a given element of G and H is a given subgroup of G.

To prove that xHx^{-1} is a subgroup of G.

Since $e \in H$, therefore at least $xex^{-1} = e \in xHx^{-1}$ and so $xHx^{-1} \neq \varnothing$.

Now let xh_1x^{-1}, xh_2x^{-1} be any two elements of xHx^{-1}. Then $h_1, h_2 \in H$.

We have $(xh_1x^{-1})(xh_2x^{-1})^{-1} = xh_1x^{-1}(x^{-1})^{-1}h_2^{-1}x^{-1}$

$= xh_1x^{-1}xh_2^{-1}x^{-1} = xh_1 eh_2^{-1}x^{-1} = xh_1h_2^{-1}x^{-1} \in xHx^{-1}$

since $h_1h_2^{-1} \in H$, H being a subgroup of G.

Thus $xh_1x^{-1}, xh_2x^{-1} \in xHx^{-1} \Rightarrow (xh_1x^{-1})(xh_2x^{-1})^{-1} \in xHx^{-1}$. Hence xHx^{-1} is a subgroup of G.

Problem 10: *Show that all those elements of an abelian group G which satisfy the relation $a^2 = e$ constitute a subgroup of G.*

Solution: Let G be an abelian group and let

$$H = \{x \in G : x^2 = e\}.$$

To prove that H is a subgroup of G.

Since $e \in G$ is such that $e^2 = e$, therefore at least $e \in H$ and so $H \neq \varnothing$.

Now let $a, b \in H$ so that $a^2 = e, b^2 = e$, *i.e.*, $a = a^{-1}$ and $b = b^{-1}$.

We have $(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1}$ [$\because$ G is abelian $\Rightarrow b^{-1}a = ab^{-1}$]

$= a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = ee = e.$

$\therefore$ By def. of H, $ab^{-1} \in H$.

Thus $a \in H, b \in H \Rightarrow ab^{-1} \in H$. Hence H is a subgroup of G.

Problem 11: *Show that a group can never be expressed as the union of two of its proper subgroups.*

Solution: Let G be a group and let $G = H \cup K$ where H and K are proper subgroups of G.

We know that the union of two subgroups is a subgroup if and only if one is contained in the other.

Since H and K are subgroups of G and $H \cup K = G$ is also a subgroup of G, therefore either $H \subseteq K$ or $K \subseteq H$. But then either $H \cup K = K$ or $H \cup K = H$, *i.e.*, either $K = G$ or $H = G$.

But this is against our hypothesis that both H and K are proper subgroups of G.

Hence our initial assumption is wrong and G cannot be expressed as the union of two of its proper subgroups.

Problem 12: *Prove that those elements of a group G which commute with the square of a given element b of G form a subgroup H of G and those which commute with b itself form a subgroup of H.*

Solution: Let $H = \{x \in G : xb^2 = b^2 x\}$. Then to prove that H is a subgroup of G. We see that H is not empty because $eb^2 = b^2 = b^2 e \Rightarrow e \in H$.

Now let $x_1, x_2 \in H$. Then $x_1 b^2 = b^2 x_1$ and $x_2 b^2 = b^2 x_2$.

First we shall show that $x_2^{-1} \in H$. We have

$$x_2 b^2 = b^2 x_2 \quad \Rightarrow \quad x_2^{-1}(x_2 b^2) x_2^{-1} = x_2^{-1}(b^2 x_2) x_2^{-1}$$

$$\Rightarrow \quad b^2 x_2^{-1} = x_2^{-1} b^2 \quad \Rightarrow \quad x_2^{-1} \in H.$$

Now we shall show that $x_1 x_2^{-1} \in H$.

We have $x_1 x_2^{-1} b^2 = x_1 b^2 x_2^{-1}$ $[\because \ b^2 x_2^{-1} = x_2^{-1} b^2]$

$= b^2 x_1 x_2^{-1}$ $[\because \ x_1 b^2 = b^2 x_1]$

$\therefore \quad x_1 x_2^{-1} \in H.$

Thus $x_1, x_2 \in H \Rightarrow x_1 x_2^{-1} \in H \Rightarrow H$ is a subgroup of G.

Let $N = \{ y \in G : yb = by \}$.

We have $yb = by \Rightarrow (yb) b = (by) b$

$\Rightarrow \quad yb^2 = b(yb) \Rightarrow yb^2 = b(by) \Rightarrow y b^2 = b^2 y.$

Thus $y \in N \Rightarrow y \in H$. Therefore $N \subseteq H$.

Now to prove that N is a subgroup of H. Obviously N is not empty since at least $e \in N$.

Let $y_1, y_2 \in N$. Then $y_1 b = by_1$ and $y_2 b = by_2$.

We have $y_2 b = by_2 \Rightarrow y_2^{-1}(y_2 b) y_2^{-1} = y_2^{-1}(by_2) y_2^{-1}$

$\Rightarrow \ b y_2^{-1} = y_2^{-1} b.$

Now, $y_1 y_2^{-1} b = y_1 by_2^{-1} = by_1 y_2^{-1}.$

$\therefore \quad y_1 y_2^{-1} \in N.$

Thus, $y_1, y_2 \in N \Rightarrow y_1 y_2^{-1} \in N.$

$\therefore$ N is a subgroup of H.

Comprehensive Problems 2

Problem 1: *What are the left cosets and right cosets of a subgroup H of a group G ? Prove that any two left cosets of H in G are identical or have no elements in common. Show that there is a 1-1 correspondence between any two left cosets of H in G.*

Solution: For definition of left and right cosets refer article 6.

Let H be a subgroup of a group G. **Then to prove that any two left cosets of H in G are either disjoint or identical.**

Let aH and bH be two left cosets of H in G where $a, b \in G$. If aH and bH are disjoint the proof is complete. So let aH and bH be not disjoint. Then there exists at least one element, say c, such that $c \in aH$ and $c \in bH$. Let $c = ah_1$ and $c = bh_2$, where $h_1, h_2 \in H$.

Then $ah_1 = bh_2$

$\Rightarrow$ $ah_1 h_1^{-1} = bh_2 h_1^{-1} \Rightarrow ae = bh_2 h_1^{-1} \Rightarrow a = b(h_2 h_1^{-1})$.

Since H is a subgroup, therefore $h_1, h_2 \in H \Rightarrow h_2 h_1^{-1} \in H$.

Let $h_2 h_1^{-1} = h_3$.

Then $a = bh_3$.

Now $aH = bh_3 H = b(h_3 H) = bH$. [$\because h_3 \in H \Rightarrow h_3 H = H$]

$\therefore$ The two left cosets aH and bH are identical if they are not disjoint. Thus either $aH \cap bH = \varnothing$ or $aH = bH$.

Now it remains to prove that there is a one-to-one correspondence between any two left cosets of H in G.

Let aH and bH be any two left cosets of H in G where $a, b \in G$. We have to show that there exists a one-to-one mapping of aH onto bH.

Let $f : aH \Rightarrow bH$ be defined by $f(ah) = bh \ \forall h \in H$.

The mapping f is **one-to-one.** If $h_1, h_2 \in H$, then $ah_1, ah_2 \in aH$. Also by def. of f, we have

$f(ah_1) = bh_1$ and $f(ah_2) = bh_2$.

Now $f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2$

$\Rightarrow$ $h_1 = h_2$ [By left cancellation law in G]

$\Rightarrow$ $ah_1 = ah_2$.

$\therefore$ the mapping f is one-to-one.

The mapping f is **onto.** Let bh' be any arbitrary element of bH.

Then $bh' \in bH \Rightarrow h' \in H \Rightarrow ah' \in aH$. Now $f(ah') = bh'$, by def. of the mapping f.

Thus $bh' \in bH \Rightarrow$ there exists $ah' \in aH$ such that $f(ah') = bh'$.

Therefore the mapping f is onto bH.

Hence the mapping f gives a one-to-one correspondence between aH and bH.

Problem 2: *Correct the following statement :*

If G is a group and H is a subgroup of G, then o (H) is a divisor of o (G).

Solution: The corresponding correct statement is :

If G is any finite group and H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.

Problem 3: *Answer the following questions :*

(*i*) *What is the order of the group* P_4 ?

(*ii*) *What is the order of the group* A_4 ?

(*iii*) *Is* A_4 *a subgroup of* P_4 ? *If yes, what is the index of* A_4 *in* P_4 ?

Solution: (i) The group P_4 is the symmetric group of permutations on a set containing four symbols, say, the set $S = \{a, b, c, d\}$.

The order of the group P_4 is the number of distinct permutations on the set $S = \{a, b, c, d\}$ and is $4!$ *i.e.*, 24.

(ii) The order of the alternating group A_4 is equal to the number of even permutations in the group P_4 and is $\frac{1}{2} \cdot 4!$ *i.e.*, 12.

(iii) Yes, A_4 is a subgroup of P_4.

We have $A_4 \subset P_4$, where P_4 is a finite group. Also if $f, g \in A_4$, then $f\ g \in A_4$. Hence A_4 is closed with respect to the operation of the group P_4 and so A_4 is a subgroup of P_4.

The index of A_4 in $P_4 = \frac{o(P_4)}{o(A_4)} = \frac{24}{12} = 2.$

Problem 4: *Let G be the group of integers under addition and let N be the set of all integral multiples of* 3. *Prove that N is a subgroup of G and determine all the cosets of N in G.*

Solution: We have $N = \{3x : x \in G$, where G is the set of integers$\}$.

To prove that N is a subgroup of the additive group of integers G.

Let $a = 3r$ and $b = 3s$ be any two elements of N where r and s are some integers.

Then $a - b = 3r - 3s = 3(r - s) \in N$ because $r - s$ is also some integer.

Thus $a \in N, b \in N \Rightarrow a - b \in N$. Hence N is a subgroup of G.

Now let us form all the cosets of N in G.

Since the group G is abelian, any right coset of N in G will be equal to the corresponding left coset. Thus there is no distinction between right and left cosets. Let us form the right cosets of N in G.

We have $N = \{..., -9, -6, -3, 0, 3, 6, 9, 12, ...\}$.

Now $0 \in G$ and $N + 0 = \{..., -9, -6, -3, 0, 3, 6, 9, 12, ...\} = N$.

Again $1 \in G$ and $N + 1 = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$.

Next $2 \in G$ and $N + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$.

We see that the right cosets N, $N + 1$ and $N + 2$ are all distinct and they are mutually disjoint *i.e.*, any two of them have no element common.

Now $3 \in G$ and $N + 3 = \{..., -9, -6, -3, 0, 3, 6, 9, ...\} = N$.

Similarly we can see that $N + 4 = N + 1$, $N + 5 = N + 2$, etc.

Thus there are only three distinct right cosets of N in G, namely N, $N + 1$, $N + 2$.

We have $G = N \cup (N + 1) \cup (N + 2)$.

Problem 5: *Let G be a finite group, $a \in G$; show that the order of a equals the order of the subgroup H of G generated by a. Hence or otherwise deduce that $o(a)$ divides $o(G)$.*

Solution: The subgroup H of G generated by a is given by

$$H = \{a^r : r \in I \text{ where } I \text{ is the set of integers}\}.$$

Let $o(H) = m$. Then proceeding as in corollary 1 of article 10, show that H has exactly m distinct elements $a, a^2, a^3, ..., a^m = e$. First show that these m elements are all distinct and then show that every element of H is equal to one of these m elements.

$\therefore \qquad o(H) = o(a) = m.$

By Lagrange's theorem $o(H)$ is a divisor of $o(G)$. Hence $o(a)$ is a divisor of $o(G)$.

Problem 6: *Consider two subgroups* $H = \{I, (1\,2)\}$ *and* $K = \{I, (1\,3)\}$ *of the symmetric group* S_3. *Determine* HK. *Using Lagrange's theorem or otherwise prove that* HK *is not a subgroup of* S_3.

Solution: Let $S = \{1, 2, 3\}$. Then the symmetric group S_3 of all the permutations on the set S has the following six members.

I (*i.e.*, identity permutation on S), (12), (23), (13), (123) and (132).

$H = \{I, (12)\}$ and $K = \{I, (13)\}$ are two subgroups of S_3.

We have $HK = \{hk : h \in H,\ k \in K\}$

$= \{(I)(I), I(13), (12)I, (12)(13)\} = \{I, (13), (12), (123)\}$.

Now $HK \subset S_3$. The number of elements in HK is 4 and $o(S_3)$ is 6. By Lagrange's theorem the order of every subgroup of a finite group must divide the order of the group. Since 4 is not a divisor of 6, therefore HK cannot be a subgroup of S_3.

Problem 7: *If a finite group G contains an element of even order, show that G must also be of even order.*

Solution: Let G be a finite group of order n.

Let $a \in G$ and $o(a) = m$, where m is even.

Let $H = \{a^r : r \in \mathbf{I}\}$ be the subgroup of G generated by a. Then

$o(H) = o(a) = m$.

By Lagrange's theorem $o(H)$ is a divisor of $o(G)$.

$\therefore$ m is a divisor of n.

Since m is even, therefore n must also be even.

Hence the group G must also be of even order.

Problem 8: *If a finite group possesses an element of order* 2, *prove that it possesses an odd number of such elements.*

Solution: Let G be a finite group of order n. Let $a \in G$ and $o(a) = 2$. Since the order of each element of a finite group divides the order of the group, therefore 2 must be a divisor of n. So n is even and thus the group G is of even order.

Now suppose G possesses m elements of order 2 and let m be even.

If a is an element of order 2, then $a^2 = e \Rightarrow aa = e \Rightarrow a = a^{-1}$. Thus an element of order 2 is its own inverse. Also the identity element e is its own inverse. Therefore the number of elements in G which are their own inverse is $m + 1$ and is odd.

$\therefore$ The number of elements in G which are not their own inverse $= n - (m + 1)$ and is also odd because n is even.

Now in a group every element possesses a unique inverse. Also if b is the inverse of c, then c is the inverse of b. Therefore $n - (m + 1)$ elements of G must be divided into pairs of two such that each pair consists of an element and its inverse. But we cannot do so because the odd integer $n - (m + 1)$ is not divisible by 2. Hence our initial assumption that m is even is wrong.

Hence G must possess an odd number of elements of order 2.

Problem 9: *Use Lagrange's theorem to show that any group of prime order can have no proper subgroups.*

Solution: Let G be a group of prime order p. Let H be a subgroup of G and let $o(H) = m$. By Lagrange's theorem $o(H)$ is a divisor of $o(G)$.

$\therefore$ m is a divisor of p.

Since p is prime, therefore either $m = 1$ or $m = p$.

Now $m = 1 \Rightarrow o(H) = 1 \Rightarrow H = \{e\}$ and $m = p \Rightarrow o(H) = o(G) \Rightarrow H = G$.

Thus either $H = \{e\}$ or $H = G$ *i.e.*, H is not a proper subgroup of G.

Hence a group of prime order can have no proper subgroups.

Problem 10: *Show that the set of the inverses of the elements of a right coset is a left coset.*

Solution: Suppose Ha is a right coset of H in G where $a \in G$.

Let ha be any element of Ha, where $h \in H$.

We have $(ha)^{-1} = a^{-1} h^{-1}$.

Since H is a subgroup, therefore $h \in H \Rightarrow h^{-1} \in H$.

$\therefore$ $a^{-1} h^{-1} \in a^{-1} H$.

Thus the inverses of all the elements of Ha belong to the left coset $a^{-1} H$. Hence

$$(Ha)^{-1} \subseteq a^{-1} H.$$

Conversely, let $a^{-1} h$ be any element of $a^{-1} H$.

Then $a^{-1} h = a^{-1} (h^{-1})^{-1} = (h^{-1} a)^{-1} \in (Ha)^{-1}$,

since $h^{-1} \in H$ and therefore $h^{-1} a \in Ha$.

Therefore every element of $a^{-1} H$ belongs to the set of the inverses of the elements of Ha.

$\therefore$ $a^{-1} H \subseteq (Ha)^{-1}$.

Hence $(Ha)^{-1} = a^{-1} H$.

Problem 11: *Given that $G = H \cup Ha_2 \cup Ha_3 \cup \ldots \cup Ha_k$ is the right coset decomposition of G relative to the subgroup H, show that $G = H \cup a_2^{-1} H \cup a_3^{-1} H \cup \ldots \cup a_k^{-1} H$ is a left coset decomposition of G relative to the subgroup H.*

Solution: We know that two right cosets of H in G are either disjoint or identical. Therefore if there are two equal right cosets in the given right coset decomposition of G, then one of them can be omitted. So let us assume that all the right cosets in the given right coset decomposition of G relative to H are distinct. Then there are k distinct right cosets of H in G. But the number of distinct right cosets of H in G is equal to the number of distinct left cosets of H in G. Therefore there are k distinct left cosets in the left coset decomposition of G relative to H.

Now we know that two right cosets Ha and Hb are distinct if and only if the two left cosets $a^{-1} H$ and $b^{-1} H$ are distinct. Since the right cosets $H, Ha_2, \ldots, Ha_k$ are all distinct, therefore the left cosets $H, a_2^{-1} H, \ldots, a_k^{-1} H$ are all distinct. Since they are k in number, therefore they are the only distinct left cosets of H in G. Now the union of all the distinct left cosets of H in G is equal to G. Hence

$$G = H \cup a_2^{-1} H \cup a_3^{-1} H \cup \ldots \cup a_k^{-1} H$$

is a left coset decomposition of G relative to the subgroup H.

Problem 12: *If $H \subseteq K$ are two subgroups of a finite group G, then show that*

$$[G : H] = [G : K][K : H].$$

Solution: Since $H \subseteq K$ are two subgroups of a group G, therefore H is also a subgroup of

Now H is a subgroup of a finite group G. Therefore by Lagrange's theorem

$$[G : H] = \frac{o(G)}{o(H)} = \frac{o(G)}{o(K)} \cdot \frac{o(K)}{o(H)} = [G : K][K : H].$$

Problem 13: *Let H and K be two subgroups of a group G. Show that any coset relative to $H \cap K$ is the intersection of a coset relative to H with a coset relative to K.*

Solution: Let a be any element of G. Then $(H \cap K)a$ is any right coset of G relative to the subgroup $H \cap K$. We shall prove that

$$(H \cap K)a = (Ha) \cap (Ka).$$

We have $(H \cap K) \subseteq H \Rightarrow (H \cap K)a \subseteq Ha$

and $(H \cap K) \subseteq K \Rightarrow (H \cap K)a \subseteq Ka.$

$\therefore$ $(H \cap K)a \supseteq Ha \cap Ka.$ ...(1)

Again let x be any element of $Ha \cap Ka$. Then $x \in Ha$ and $x \in Ka$.

$\therefore$ $x = ha = ka$ for some $h \in H, k \in K$.

$\therefore$ $xa^{-1} = h = k.$

$\therefore$ $xa^{-1} \in H \cap K \Rightarrow (xa^{-1})a \in (H \cap K)a \Rightarrow x \in (H \cap K)a.$

Consequently $Ha \cap Ka \subseteq (H \cap K)a.$ ...(2)

From (1) and (2), we conclude that $(H \cap K)a = Ha \cap Ka$.

A similar proof can be given in the case of a left coset.

Problem 14: *Prove that the intersection of two subgroups, each of finite index, is again of finite index.*

Solution: Let H and K be two subgroups of a group G. Let $[G : H] = m$ and $[G : K] = n$. Let $Ha_1, ..., Ha_m$ and $Kb_1, ..., Kb_n$ be the distinct right cosets of H and K respectively. We are to show that the number of distinct right cosets of $H \cap K$ in G is finite. Let $(H \cap K)a$ be any right coset of $H \cap K$ in G. Then it can be easily shown that $(H \cap K)a = Ha \cap Ka$. Thus each right coset of $H \cap K$ is given by the intersection of a right coset of H and a right coset of K. Since the number of distinct right cosets of H is m and the number of distinct right cosets of K is n, therefore the number of distinct right cosets of $H \cap K$ can be at most equal to mn. Hence $H \cap K$ is of finite index in G.

Comprehensive Problems 3

Problem 1: *Prove that any group is isomorphic to a transformation group.*

Solution: Let G be any group, the operation denoted multiplicatively.

If f is a one-one mapping of G onto G, then f is called a transformation of G.

So we have to show that the group G is isomorphic to a group of one-to-one mappings of G onto G.

Now give the same proof as given in Cayley's theorem in article 12.

Problem 2: *Find the regular permutation group isomorphic to the group* $(\{1, \omega, \omega^2\}, \bullet)$.
(Meerut 2006B)

Solution: Let G denote the multiplicative group $(\{1, \omega, \omega^2\}, \bullet)$. By Cayley's theorem the group G is isomorphic to a permutation group G' called the regular permutation group of G. This group G' consists of the following three permutations f_1, f_2, f_3 :

$$f_1 = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1.1 & 1.\omega & 1.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega & \omega^2 \end{pmatrix} = \text{identity permutation}$$

$$f_2 = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega.1 & \omega.\omega & \omega.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega & \omega^2 & 1 \end{pmatrix} = (1 \quad \omega \quad \omega^2)$$

$$f_3 = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2.1 & \omega^2.\omega & \omega^2.\omega^2 \end{pmatrix} = \begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \end{pmatrix} = (1 \quad \omega^2 \quad \omega).$$

Hence the regular permutation group isomorphic to the group $(\{1, \omega, \omega^2\}, \bullet)$ consists of the three permutations

$$I, (1 \quad \omega \quad \omega^2) \quad \text{and} \quad (1 \quad \omega^2 \quad \omega).$$

Problem 3: ***Fermat's Theorem:*** *If p is a prime number and a is any integer, prove that* $a^p \equiv a (\text{mod}_p)$.

Solution: Proceed as in article 10, in Corollary 4.

Hints to Objective Type Questions

Multiple Choice Questions

1. The index of H in G is the number of distinct right (left) cosets of H in G. Here, $H, H + 1, H + 2, H + 3, H + 4$ are the only distinct right cosets of H in G and their number is 5. So, the index of H in G is 5.
   Also, see Illustration 1 after article 6.
2. By Lagrange's theorem, the index of A_4 in
$$P_4 = \frac{o(P_4)}{o(A_4)} = \frac{4!}{\frac{1}{2} \cdot (4!)} = \frac{24}{12} = 2.$$
3. See article 2, Theorem 1.
4. See article 2, Theorem 2.
5. See article 4, Theorem 1.
6. See article 10.
7. See article 6, Theorem 1.
8. See article 3, Theorem 3 (Corollary).

9. See article 10.
10. See article 3, Theorem 2.
11. See article 2, Theorem 2.
12. See article 5.
13. See Illustration 1 after article 1.
14. See article 5, Theorem 1.
15. See Illustration 1 after article 6.
16. See article 12.
17. See article 10, Corollary 4.
18. See Problem 3(i) of Comprehensive Problems 2.
19. See Problem 3(ii) of Comprehensive Problems 2.
20. See Problem 6 of Comprehensive Problems 2.

Fill in the Blank(s)

1. See article 1.
2. See article 4, Theorem 1.
3. See article 6, Theorem 5.
4. See the definition of index of a subgroup in a group, in article 8.
5. See article 10, Corollary 2.
6. See article 12, Cayley's theorem.

True or False

1. See an Important Note and Illustration 1 after theorem 3 of article 3.
2. See Theorem of article 1.
3. See Note of article 10, Corollary 2.
4. See article 5, Note 2.
5. See article 11.

○○○

Chapter-7

Cyclic Groups

Comprehensive Problems 1

Problem 1: *Show that any two cyclic groups of the same order are isomorphic.*

Solution: Let $G = (a)$ and $G' = (b)$ be two cyclic groups of the same order generated by a and b respectively. To prove $G \cong G'$.

Case I: The groups G and G' are finite, say each of order n. Then $o(a) = n$ and $o(b) = n$.

Also $G = \{a^0 = e, a, a^2, ..., a^{n-1}\}$

and $G' = \{b^0 = e', b, b^2, ..., b^{n-1}\}$,

where e and e' are the identities of the groups G and G' respectively.

Consider the mapping $f : G \to G'$ defined by

$$f(a^r) = b^r, \text{ where } 0 \le r \le n-1.$$

The mapping f is one-one. Since

$$f(a^r) = f(a^s), \text{ where } 0 \le r \le n-1, 0 \le s \le n-1$$

$$\Rightarrow \quad b^r = b^s \Rightarrow r = s \quad [\because \text{ the elements } b^0, b, ..., b^{n-1} \text{ are all distinct}]$$

$$\Rightarrow \quad a^r = a^s.$$

Again the number of elements in G is equal to the number of elements in G'. Therefore f is one-one implies f must be onto G'.

Finally $f(a^r a^s) = f(a^{r+s}) = f(a^{nu+k})$, where u is some integer and $0 \le k < n$

$$= f(a^{nu} a^k) = f[(a^n)^u a^k]$$

$$= f(a^k) \qquad [\because a^n = e]$$

$$= b^k = (b^n)^u b^k \qquad [\because b^n = e']$$

$$= b^{nu+k} = b^{r+s} = b^r b^s = f(a^r) f(a^s).$$

Therefore f preserves compositions in G and G' and so f is an isomorphism of G onto G'. Hence $G \cong G'$.

Case II: The groups G and G' are infinite cyclic groups. In this case distinct integral powers of a will give distinct elements of G and distinct integral powers of b will give distinct elements of G'. Thus

$$G = \{..., a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, ...\}$$

and $G' = \{..., b^{-3}, b^{-2}, b^{-1}, b^0 = e', b, b^2, b^3, ...\}$.

Consider the mapping $f : G \to G'$ defined by

$$f(a^r) = b^r, \ \forall \ r \in \mathbf{I}, \mathbf{I} \text{ being the set of integers.}$$

The mapping f is one-one because

$$f(a^r) = f(a^s) \Rightarrow b^r = b^s \Rightarrow r = s \Rightarrow a^r = a^s.$$

Also f is onto G' because if b^r is any element of G', then there exists $a^r \in G$ such that $f(a^r) = b^r$.

Again $$f(a^r a^s) = f(a^{r+s}) = b^{r+s} = b^r b^s = f(a^r)\, f(a^s).$$

Hence f is an isomorphism of G onto G' and consequently

$$G \cong G'.$$

Problem 2: *Show that all finite cyclic groups of order n are isomorphic to the additive group of integers modulo n.*

Solution: Let $G = (a)$ be a finite cyclic group of order n generated by a. Then

$$o(a) = n$$

and $$G = \{a^0 = e, a, a^2, ..., a^{n-1}\}.$$

Let $G' = (\{0, 1, 2, ..., n-1\}, +_n)$ be the additive group of integers modulo n.

To prove $$G \cong G'.$$

Consider the mapping $f : G \to G'$ defined by $f(a^r) = r$, where $0 \le r \le n-1$.

The mapping f is one-one. Since

$$f(a^r) = f(a^s), \text{where } 0 \le r \le n-1, 0 \le s \le n-1$$

$\Rightarrow$ $$r = s \Rightarrow a^r = a^s.$$

Also the number of elements in G is equal to the number of elements in G'. Therefore f is one-one implies f must be onto G'.

Finally $f(a^r a^s) = f(a^{r+s}) = f(a^{nu+k})$, where u is some integer and $0 \le k < n$

$$= f(a^{nu} a^k) = f[(a^n)^u a^k]$$
$$= f(e^u a^k) = f(ea^k)$$
$$= f(a^k) = k = r +_n s$$
$$[\because\ r + s = nu + k, \text{where } 0 \le k < n \text{ implies that } r +_n s = k]$$
$$= f(a^r) +_n f(a^s).$$

Thus, the mapping f preserves compositions in G and G'.

Hence f is an isomorphism of G onto G' and consequently

$$G \cong G'.$$

Problem 3: *Find the order of each element in the multiplicative group of residues* 1, 2, 3, 4, 5, 6 *prime to* 7. *Show that the group is cyclic of order* 6 *and that it can be generated by* 3 *and* 5 *and not by any of the other elements.*

Solution: Let $G = (\{1, 2, 3, 4, 5, 6\}, \times_7)$ be the multiplicative group of the residues 1, 2, 3, 4, 5, 6 modulo 7.

The identity of the group G is 1 and so $o(1) = 1$.

Now $2^1 = 2, 2^2 = 2 \times_7 2 = 4, 2^3 = 2 \times_7 2 \times_7 2 = 4 \times_7 2 = 1$, *i.e.*, the identity element.

$\therefore$ $$o(2) = 3.$$

Since $2 \times_7 4 = 1 = 4 \times_7 2$, therefore the inverse of 2 in the group G is 4.
Now we know that in any group G, $o(a) = o(a^{-1})$.

$\therefore$ $o(4) = o(2) = 3$.

Again $3^1 = 3, 3^2 = 3 \times_7 3 = 2, 3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6,$

$3^4 = 6 \times_7 3 = 4, 3^5 = 4 \times_7 3 = 5,$

$3^6 = 3^5 \times_7 3 = 5 \times_7 3 = 1$, *i.e.*, the identity element.

$\therefore$ $o(3) = 6$.

Also $3 \times_7 5 = 1 = 5 \times_7 3$.

Therefore the inverse of 3 in the group G is 5 and so $o(5) = o(3) = 6$.

Again $6^1 = 6, 6^2 = 6 \times_7 6 = 1$ *i.e.*, the identity element.

$\therefore$ $o(6) = 2$.

Thus in the group G, we have

$$o(1) = 1, o(2) = 3, o(3) = 6, o(4) = 3, o(5) = 6, o(6) = 2.$$

Now the order of the group G is 6. The element $3 \in G$ is also of order 6. Thus $o(3) = o(G)$ and so G is a cyclic group generated by 3. We can write

$$G = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}.$$

The element 5 of G is also of order 6. Therefore 5 is also a generator of G.

Now the order of no other element of G except 3 and 5 is equal to the order of the group G. Therefore no other element of G except 3 and 5 can be a generator of G.

Problem 4: *"A group may be isomorphic to one of its proper subgroups". Either disprove this statement or give an example to prove it.*

Solution: It is possible that a group may be isomorphic to one of its proper subgroups as shown in the following example :

Let $G = (\{..., -3, -2, -1, 0, 1, 2, 3, ...\}, +)$

be the additive group of integers.

Consider the subgroup

$$H = \{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$$

of G. Then H is a proper subgroup of G.

Let $f : G \to H$ be defined by

$$f(x) = 2x, \ \forall \ x \in G.$$

Then f is an isomorphism of G onto H and so

$$G \cong H.$$

Hence a group may be isomorphic to one of its proper subgroups.

Problem 5: *Define a cyclic group. Prove that a cyclic group G with a generator a of finite order n has exactly n distinct elements.*

Solution: **Cyclic group: Definition:** *Let G be a group, the operation denoted multiplicatively. If there exists an element a in G such that each element of G can be expressed as some integral power of a, then G is said to be a cyclic group generated by a.*

Let $G = (a)$ be a cyclic group generated by a and let $o(a) = n$. Then to show that $o(G) = n$ *i.e.*, G has exactly n distinct elements.

We have $G = \{a^r : r \in \mathbf{I}\}$ *i.e.*,

$$G = \{..., a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, ...\}.$$

First we show that the n elements

$$a, a^2, a^3, ..., a^n = e = a^0 \qquad ...(1)$$

of G are all distinct.

No two of the n elements given in (1) can be equal. For if possible, let

$$a^r = a^s, 1 \le s < r \le n.$$

Then $a^r = a^s \Rightarrow a^r a^{-s} = a^s a^{-s} \in a^{r-s} = a^{s-s} = a^0 = e.$

Since $0 < r - s < n$, therefore $a^{r-s} = e$ implies that the order of a is less than n which is against hypothesis. Hence $a^r \neq a^s$ *i.e.*, the n elements of G given in (1) are all distinct.

Now we shall show that every element of G is equal to one of the n elements given in (1).

Let a^t be any element of G where t is any integer. By division algorithm, there exist two integers q and r such that

$$t = nq + r, \text{ where } 0 \le r < n.$$

$$\therefore \quad a^t = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

Since $0 \le r < n$, therefore a^r is one of the n elements given in (1).

Hence if G is a cyclic group generated by a and $o(a)$ is n, then G has exactly n distinct elements $a, a^2, a^3, ..., a^n = e$. Thus if G is a cyclic group generated by a, then $o(G) = o(a)$.

Problem 6: *Give an example of an infinite non-abelian group and one example of an abelian group which is not cyclic.*

Solution: **Example of an infinite non-abelian group:** Let M be the set of all 2×2 non-singular matrices having their elements as real numbers. Then M is an infinite group with respect to matrix multiplication. Also this group is non-abelian because if we take the two members $A = \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix}$ of M, we find that $AB = \begin{bmatrix} 5 & 18 \\ 8 & 26 \end{bmatrix}$ and $BA = \begin{bmatrix} 8 & 18 \\ 11 & 23 \end{bmatrix}$.

Thus $AB \neq BA$ and so the operation of multiplication of matrices on the set M is not commutative. Hence the group M is non-abelian.

Example of an abelian group which is not cyclic: Give the example of the group of order 4 given in solved example 50 which is abelian but not cyclic.

Problem 7: *If ω be an imaginary cube root of unity, show that the set $\{1, \omega, \omega^2\}$ is a cyclic group of order 3 with respect to multiplication.* **(Kanpur 2009, 10; Bundelkhand 14)**

Solution: Let $G = \{1, \omega, \omega^2\}$.

To show that G is a group with respect to multiplication see problem 2 of Comprehensive Problems 3, Chapter Groups.

The number of distinct elements in G is 3, therefore $o(G) = 3$.

Now $\omega^1 = \omega$, $\omega^2 = \omega^2$, $\omega^3 = 1$, *i.e.*, identity of G. Therefore $o(\omega) = 3 = o(G)$.

Hence G is a cyclic group generated by ω. Note that ω generates each element of G because we can write

$$G = \{\omega, \omega^2, \omega^3 = 1\}.$$

Problem 8: *Prove that a non-commutative group has at least six elements.*

Solution: To prove that a non-commutative group has at least six elements, we have to prove that every group of order less than six must be abelian and there is at least one group of order 6 which is non-abelian.

For the first part proceed as in example 5. Now to show that there is at least one group of order six which is non-abelian. Consider the symmetric group P_3 of permutations on three symbols a, b, c. The order of the group P_3 is $3!$ *i.e.*, 6 and we know that it is a non-abelian group.

Hence a non-commutative group has at least six elements.

Problem 9: *What is the least order of a non-abelian group? Show that all proper subgroups of a group of order* 8 *must be abelian.*

Solution: The least order of a non-abelian group is six because every group of order less than six is always abelian.

Let G be a group of order 8 and H be a proper subgroup of G. Then $1 < o(H) < 8$. By Lagrange's theorem $o(H)$ must be a divisor of $o(G)$. Therefore $o(H)$ can be 2 or 4. But every group of order 2 or 4 is abelian. Hence H must be abelian.

Problem 10: *Show that the group* $(\{1, 2, 3, 4\}, \times_5)$ *is cyclic.*

Solution: Let G denote the given group $(\{1, 2, 3, 4\}, \times_5)$. The order of the group G is 4. If there exists an element $a \in G$ such that $o(a) = o(G) = 4$, then the group G will be cyclic and a will be a generator of G.

So let us find the orders of the elements of the group G. The identity of the group G is 1 and so $o(1) = 1$.

Now, $2^1 = 2, 2^2 = 2 \times_5 2 = 4, 2^3 = 2 \times_5 2 \times_5 2 = 4 \times_5 2 = 3,$

$2^4 = 2^3 \times_5 2 = 3 \times_5 2 = 1$ *i.e.*, the identity.

$\therefore \quad o(2) = 4 = o(G)$.

Hence G is a cyclic group and 2 is a generator of G. We observe that 2 generates each element of G.

Problem 11: *Show that the residue classes* $\{1\}, \{3\}, \{5\}, \{7\}$ *modulo* 8 *form a multiplicative group. Is this a cyclic group ?*

Solution: Let $G = \{1\}, \{3\}, \{5\}, \{7\}$. To show that G is a group for multiplication of residue classes modulo 8. The composition table for G for multiplication of residue classes modulo 8 is as given below :

$\times_8$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Closure property: We see that all the entries in the composition table are elements of the set G. Therefore G is closed with respect to multiplication of residue classes modulo 8.

Associativity: The operation of multiplication of residue classes modulo 8 is associative on the set G. For if $\bar{a}, \bar{b}, \bar{c}$ are any three elements of G, then

$$\bar{a}\,(\bar{b}\,\bar{c}) = \bar{a}\,\overline{bc} = \overline{a\,(bc)} = \overline{(ab)\,c} = \overline{ab}\;\bar{c} = (\bar{a}\,\bar{b})\,\bar{c}.$$

Existence of identity: We have $\bar{1} \in G$. If $\bar{a}$ is any element of G, then $\bar{1}\,\bar{a} = \overline{1a} = \bar{a} = \bar{a}\,\bar{1}$. Therefore $\bar{1}$ is the identity.

Existence of inverse: From the table we see that the inverses of $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ are $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ respectively. Thus each element of G has its inverse in G.

Hence G is a group for multiplication of residue classes modulo 8.

Now to see whether the group G is cyclic or not, let us find the orders of the elements of G.

We have $o(\bar{1}) = 1$ because $\bar{1}$ is the identity of G.

Also $(\bar{3})^2 = (\bar{3})(\bar{3}) = \bar{9} = \bar{1}$,

i.e., identity and so $o(\bar{3}) = 2$.

Similarly $(\bar{5})^2 = (\bar{5})(\bar{5}) = \overline{25} = \bar{1}$ and $(\bar{7})^2 = (\bar{7})(\bar{7}) = \overline{49} = \bar{1}$.

$\therefore$ $o(\bar{5}) = 2$ and $o(\bar{7}) = 2$.

We see that there is no element in G whose order is equal to the order of the group G. Hence the group G is not cyclic.

Problem 12: *How many generators are there of the cyclic group of order* 10 ?

(Meerut 2005)

Solution: Let G be a cyclic group of order 10 generated by a. Then $o(a) = o(G) = 10$.

We can write

$$G = \{a, a^2, a^3, a^4, ..., a^8, a^9, a^{10} = e\}.$$

We know that if G is a cyclic group generated by a and $o(a) = n$, then a^m is a generator of G if and only if m and n are relatively prime *i.e.*, the H.C.F. of m and n is 1. So we make the following observations:

1 and 10 are relatively prime, 3 and 10 are relatively prime, 7 and 10 are realtively prime, 9 and 10 are relatively prime. Therefore a^1 *i.e.*, a, a^3, a^7 and a^9 are all generators of G.

Since 2 and 10, 4 and 10, 5 and 10, 6 and 10, 8 and 10, 10 and 10 are not relatively prime, therefore none of the elements a^2, a^4, a^5, a^6, a^8 and a^{10} can be a generator of G.

Hence G has only four generators a, a^3, a^7 and a^9.

Problem 13: *How many elements of the cyclic group of order 6 can be used as generators of the group ?*

Solution: Proceed as in problem 12.

Here $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$.

Also $o(a) = o(G) = 6$.

Since 1 and 6 are relatively prime and 5 and 6 are relatively prime, therefore a^1, *i.e.*, a and a^5 are generators of G.

Again 2 and 6, 3 and 6, 4 and 6, 6 and 6 are not relatively prime. Therefore none of the elements a^2, a^3, a^4 and a^6 can be a generator of G.

Problem 14: *Prove that each element $b \neq e$ in an infinite cyclic group (a) is of infinite order.*

Solution: Let $G = (a)$ be an infinite cyclic group generated by a. Then the order of the element a in the group G is zero or infinite.

Let $b \in G$ and $b \neq e$. Then $b = a^r$, where r is some non-zero integer.

Suppose $o(b)$ is finite and is equal to n.

Then $o(b) = n \Rightarrow b^n = e \Rightarrow (a^r)^n = e \Rightarrow a^{rn} = e$.

Also $a^{rn} = e \in (a^{rn})^{-1} = e^{-1} \Rightarrow a^{-rn} = e$.

Now one of rn and $-rn$ is a positive integer. Therefore $a^{rn} = e = a^{-rn} \Rightarrow$ order of a is finite and so a cannot be a generator of an infinite cyclic group. Hence our assumption that $o(b)$ is finite is wrong.

Therefore each element $b \neq e$ in an infinite cyclic group is of infinite order.

Hints to Objective Type Questions

Multiple Choice Questions

1. The order of the multiplicative cyclic group $\{1, \omega, \omega^2\}$ is 3. We have $o(1) = 1$, $o(\omega) = 3$ and $o(\omega^2) = 3$. We know that an element of a cyclic group is a generator of the group if and only if its order is equal to the order of the group. So, ω and ω^2 are the only generators of the given group.
2. See example 3 after article 2.
3. See article 1, Illustration 1.
4. See article 1, Illustration 4.
5. See example 1 after article 2.
6. See example 2 after article 2.
7. See article 2, Theorem 1.
8. See article 1, Illustration 1.
9. A group of rational numbers under multiplication is not cyclic.

10. The generator of the cyclic group $(\{0,1,2,3\}, +_4)$ is 1.
We have $1^1 = 1, 1^2 = 1 +_4 1 = 2, 1^3 = 1 +_4 1^2 = 3, 1^4 = 1 +_4 1^3 = 1 +_4 3 = 0.$

11. See article 2, Theorem 8, Note.

12. See Example 2, Note.
Here G consists of all symbols a^i, $i = 0,1,2,\ldots(n-1)$,
such that $a^0 = a^n = e$, $a^i a^j = a^{i+j}$ if $i + j \le n$
and $a^i a^j = a^{i+j-n}$, if $i + j > n$.

13. See article 2, Theorem 1 and Theorem 3, Corollary.

14. See Problem 12 of Comprehensive Problems 1.

15. See Problem 13 of Comprehensive Problems 1.

Fill in the Blank(s)

1. See article 2, Theorem 1.

2. See article 2, Theorem 6.

3. See article 1, Illustration 5.

4. 1 and –1 are the generators of the additive group of integers.

5. See article 2, Theorem 9.

True or False

1. See problem 8 of Comprehensive Problems 1.

2. See article 2, Theorem 2.

3. See Example 4 after article 2.

4. See article 2, Theorem 3, Corollary.

5. See article 2, Theorem 5.

❍❍❍

Chapter-8

Normal Subgroups

Comprehensive Problems 1

Problem 1: *Show that a subgroup H of a group G is normal if and only if the set G / H of all its left cosets is closed under (complex) multiplication.*

Solution: Let H be a subgroup of a group G.

We have $G/H = \{ xH : x \in G \}$ *i.e.*, G/H is the family of all left cosets of H in G.

'Only if ' part: Let H be a normal subgroup of G. Let a, b be any two elements of G. Then aH and bH are two left cosets of H in G.

We have

$$(aH)(bH) = a(Hb)H = a(bH)H \quad [\because H \text{ is normal} \Rightarrow Hb = bH]$$
$$= abHH = abH. \quad [\because HH = H]$$

Since $a \in G,\ b \in G \Rightarrow ab \in G$, therefore abH is also a left coset of H in G *i.e.*, $abH \in G/H$.

Thus $aH \in G/H,\ bH \in G/H \Rightarrow (aH)(bH) \in G/H$ *i.e.*, G/H is closed under multiplication of complexes.

'If ' part: Let H be a subgroup of G such that the product of two left cosets of H in G is again a left coset of H in G *i.e.*, G/H is closed under complex multiplication. Then to prove that H is a normal subgroup of G.

Let x be any element of G. Then $x^{-1} \in G$. Therefore xH and $x^{-1}H$ are two left cosets of H in G. Consequently, by hypothesis $xHx^{-1}H$ is also a left coset of H in G. Since $e \in H$, therefore $xex^{-1} = e$ is an element of the left coset $xHx^{-1}H$. But H itself is a left coset of H in G and $e \in H$. Also if two left cosets have one element common they must be identical. Therefore we must have

$$xHx^{-1}H = H \quad \forall \quad x \in G$$

$$\Rightarrow \quad xhx^{-1}h_1 \in H \quad \forall \quad x \in G \text{ and } \forall \quad h, h_1 \in H$$

$$\Rightarrow \quad (xhx^{-1}h_1)h_1^{-1} \in Hh_1^{-1} \quad \forall \quad x \in G \text{ and } \forall \quad h, h_1 \in H$$

$$\Rightarrow \quad xhx^{-1} \in H \quad \forall \quad x \in G \text{ and } \forall \quad h \in H$$

$$[\because Hh_1^{-1} = H \text{ as } h_1 \in H \Rightarrow h_1^{-1} \in H]$$

$\Rightarrow$ H is a normal subgroup of G.

Problem 2: *Determine the coset decompositions of the subgroup $H = \{I, (12)\}$ in S_3 the permutation group of degree 3; and further show that H is not normal in S_3.*

Solution: Let $S_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$ where

$f_1 =$ identity permutation I,

$f_2 = (12),\ f_3 = (23),\ f_4 = (31),\ f_5 = (123),\ f_6 = (132).$

We have $H = \{I, (12)\} = \{ f_1, f_2 \}$.

Let us form the right cosets of H in G.

We have

$H f_1 = H$ since f_1 is the identity element of G,

$H f_2 = \{ f_1 f_2, f_2 f_2 \} = \{ f_2, f_1 \} = H$,

$H f_3 = \{ f_1 f_3, f_2 f_3 \} = \{ f_3, f_6 \}$, $[\because f_2 f_3 = (12)(23) = (132) = f_6]$

$H f_4 = \{ f_1 f_4, f_2 f_4 \} = \{ f_4, f_5 \}$, $[\because f_2 f_4 = (12)(31) = (123) = f_5]$

$H f_5 = \{ f_1 f_5, f_2 f_5 \} = \{ f_5, f_4 \}$,

$[\because f_2 f_5 = (12)(123) = (13) = (31) = f_4]$

and $H f_6 = \{ f_1 f_6, f_2 f_6 \} = \{ f_6, f_3 \}$. $[\because f_2 f_6 = (12)(132) = (23) = f_3]$

We see that $H f_1 = H f_2 = H$, $H f_3 = H f_6$ and $H f_4 = H f_5$. Thus we get only three distinct right cosets *i.e.*, $H, H f_3$ and $H f_4$.

Now let us form the left cosets of H in G.

We have $f_1 H = H$,

$f_2 H = \{ f_2 f_1, f_2 f_2 \} = \{ f_2, f_1 \} = H$,

$f_3 H = \{ f_3 f_1, f_3 f_2 \} = \{ f_3, f_5 \}$, $[\because f_3 f_2 = (23)(12) = (123) = f_5]$

$f_4 H = \{ f_4 f_1, f_4 f_2 \} = \{ f_4, f_6 \}$, $[\because f_4 f_2 = (31)(12) = (132) = f_6]$

$f_5 H = \{ f_5 f_1, f_5 f_2 \} = \{ f_5, f_3 \}$ $[\because f_5 f_2 = (123)(12) = (23) = f_3]$

and $f_6 H = \{ f_6 f_1, f_6 f_2 \} = \{ f_6, f_4 \}$.

$[\because f_6 f_2 = (132)(12) = (13) = (31) = f_4]$

We see that $f_1 H = f_2 H = H$, $f_3 H = f_5 H$ and $f_4 H = f_6 H$. Thus we get only three distinct left cosets *i.e.*, $H, f_3 H$ and $f_4 H$.

Now $H f_3 = \{ f_3, f_6 \}$ and $f_3 H = \{ f_3, f_5 \}$.

Thus $H f_3 \neq f_3 H$. Hence H is not a normal subgroup of S_3.

Problem 3: *Show that a subgroup of index 2 is always an invariant (normal) subgroup. Hence show that alternating group A_n is an invariant subgroup of S_n the symmetric group of degree n.*

(Bundelkhand 2014)

Solution: For the first part of this question see example 3.

Second part: If S_n is the symmetric group of degree n, we know that

$$o(S_n) = n!.$$

The alternating group A_n is a subgroup of S_n and

$$o(A_n) = \frac{1}{2} n!.$$

By Lagrange's theorem the index of A_n in S_n

$$= \frac{o(S_n)}{o(A_n)} = \frac{n!}{\frac{1}{2} n!} = 2.$$

By first part of this question we know that if G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G. Hence A_n is the normal subgroup of S_n.

Problem 4: *If M and N are two normal subgroups of G and $M \cap N = (e)$, then prove that for any $n \in N, m \in M$, $nm = mn$.*

Solution: Suppose that N and M are two normal subgroups of G and that $N \cap M = \{e\}$. Show that every element of N commutes with every element of M.

Let n be any element of N and m any element of M. Then to prove that $nm = mn$. Consider the element $nmn^{-1}m^{-1}$.

Since N is normal, $mn^{-1}\, m^{-1} \in N$. Also $n \in N$. Therefore $nmn^{-1}\, m^{-1} \in N$.

Again M is normal $\Rightarrow$ $n\, m\, n^{-1} \in M$. Also $m^{-1} \in M$. Therefore $nmn^{-1}\, m^{-1} \in M$.

Thus $n\, m\, n^{-1}\, m^{-1} \in N$ and $nmn^{-1}\, m^{-1} \in M \Rightarrow n\, m\, n^{-1}\, m^{-1} \in N \cap M$

$\Rightarrow$ $nmn^{-1}\, m^{-1} = e$ $[\because N \cap M = \{e\}]$

$\Rightarrow$ $n\, m = m\, n.$

Problem 5: *Let G be a group and N a subgroup of G. Prove that the following statements are equivalent :*

(i) $gng^{-1} \in N$ *for all* $g \in G, n \in N$

(ii) $gNg^{-1} = N$ *for all* $g \in G$ **(Purvanchal 2006; Kanpur 07)**

(iii) Every left coset of N in G is a right coset of N in G

(iv) Product of two right cosets of N in G is again a right coset of N in G.

Solution: (i) $\Rightarrow$ (ii).

Let $gng^{-1} \in N, \ \forall \ g \in G$ and $\forall \ n \in N$.

Then to prove that $gNg^{-1} = N, \ \forall \ g \in G$.

We have $gng^{-1} \in N, \ \forall \ g \in G$ and $\forall \ n \in N$

$\Rightarrow$ $gNg^{-1} \subseteq N, \ \forall \ g \in G.$ ...(1)

Also $g \in G \Rightarrow g^{-1} \in G$. Therefore from (1), we have

$g^{-1}N(g^{-1})^{-1} \subseteq N \ \forall \ g \in G$

$\Rightarrow$ $g^{-1}Ng \subseteq N \ \forall \ g \in G$

$\Rightarrow$ $g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1} \ \forall \ g \in G$

$\Rightarrow$ $N \subseteq gNg^{-1} \ \forall \ g \in G.$ ...(2)

From (1) and (2), we conclude that $gNg^{-1} = N$ for all $g \in G$.

$\therefore$ (i) $\Rightarrow$ (ii).

Now we shall prove that (ii) $\Rightarrow$ (iii).

Let $gNg^{-1} = N$ for all $g \in G$.

Then to show that every left coset of N in G is a right coset of N in G.

We have $gNg^{-1} = N \quad \forall \quad g \in G$

$\Rightarrow \quad (gNg^{-1})\, g = Ng \quad \forall \quad g \in G$

$\Rightarrow \quad gN = Ng$ for all $g \in G$

$\Rightarrow \quad$ every left coset gN is the right coset Ng

$\Rightarrow \quad$ every left coset of N in G is a right coset of N in G.

Hence (ii) $\Rightarrow$ (iii).

Now we shall prove that (iii) $\Rightarrow$ (iv).

Suppose that every left coset of N in G is a right coset of N in G. Then to prove that the product of two right cosets of N in G is again a right coset of N in G.

Let Na and Nb be two right cosets of N in G. By hypothesis aN is equal to some right coset of N in G. Let

$$aN = Nx, \text{ for some } x \in G.$$

Since $e \in N$, therefore $ae = a \in aN$.

$\therefore \quad a \in Nx.$ $\qquad [\because aN = Nx]$

But $\quad a \in Nx \Rightarrow Na = Nx.$

[See theorem 3 of article 6 of the chapter on Subgroups]

$\therefore \quad aN = Na.$ $\qquad [\because aN = Nx \text{ and } Nx = Na]$

Now $\quad (Na)\,(Nb) = N(aN)b = N(Na)b$ $\qquad [\because aN = Na]$

$\qquad\qquad = NNab = Nab.$ $\qquad [\because NN = N]$

Since $a \in G,\ b \in G \Rightarrow ab \in G$, therefore Nab is also a right coset of N in G. Thus the product of two right cosets Na and Nb of N in G is again the right coset Nab of N in G.

Hence (iii) $\Rightarrow$ (iv).

Finally we shall prove that (iv) $\Rightarrow$ (i).

Suppose that the product of two right cosets of N in G is again a right coset of N in G.

Then to prove that $gng^{-1} \in N, \ \forall \ g \in G$ and $\forall \quad n \in N$.

Let g be any element of G. Then $g^{-1} \in G$. Therefore Ng and Ng^{-1} are two right cosets of N in G. Consequently, by hypothesis $N\ g\ N\ g^{-1}$ is also a right coset of N in G. Since $e \in N$, therefore $e\ g\ e\ g^{-1} = e$ is an element of the right coset $N\ g\ N\ g^{-1}$. But N itself is a right coset of N in G and $e \in N$. Also if two right cosets have one element common they must be identical. Therefore we have

$$N\ g\ N\ g^{-1} = N \quad \forall \quad g \in G$$

$\Rightarrow \quad n_1\ g\ n\ g^{-1} \in N \quad \forall \quad g \in G \qquad$ and $\quad \forall \quad n_1, n \in N$

$\Rightarrow \quad n_1^{-1}(n_1\ g\ n\ g^{-1}) \in n_1^{-1}N \quad \forall\, g \in G \qquad$ and $\quad \forall \quad n_1, n \in N$

$\Rightarrow \quad g\ n\ g^{-1} \in N \quad \forall \quad g \in G \qquad$ and $\quad \forall \quad n \in N.$

$[\because \ n_1^{-1}N = N \ \text{ as } \ n_1 \in N \Rightarrow n_1^{-1} \in N]$

Hence (iv) $\Rightarrow$ (i). Thus (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

Hence the statements (i), (ii), (iii) and (iv) are equivalent.

Problem 6: *Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.*

Solution: For the first part of this question see example 4.

Now we shall give an example to show that $H \cap N$ need not be a normal subgroup of G.

Let G be the symmetric group S_4 of 4 ! permutations on four symbols a, b, c, d. Consider the following subgroups of S_4.

(i) $N = A_4$ *i.e.*, the alternating group of all even permutations in S_4.

We have $o(A_4) = \frac{1}{2} . 4 !$.

(ii) $H = \{I, (ab), (cd), (ab)(cd)\}$.

Since index of A_4 in $P_4 = \frac{o(P_4)}{o(A_4)} = \frac{4 !}{\frac{1}{2} . 4 !} = 2$, therefore A_4 is a normal subgroup of P_4.

Thus N is a normal subgroup of G.

Since in H, (ab) and (cd) are odd permutations and I and $(ab)(cd)$ are even permutations, therefore we have

$$H \cap N = \{I, (ab)(cd)\} = K, \text{ say.}$$

We shall show that K is not a normal subgroup of G.

Take the element $(abcd) \in G$ and the element $(ab)(cd) \in K$. We have

$$(abcd)(ab)(cd)(abcd)^{-1} = (abcd)(ab)(cd)(dcba)$$
$$= (ad)(bc) \in K.$$

Therefore K is not a normal subgroup of G.

Problem 7: *Give an example of each of the following :*

(i) A subgroup H of some group G, which is not normal in G.

(ii) A non-trivial subgroup H of a non-abelian group G, which is normal in G.

(Kumaun 2011, 12, 14)

Solution: Let G be the symmetric group S_3 of 3 ! permutations on three symbols 1, 2, 3 *i.e.*,

$$G = S_3 = \{I, (12), (23), (31), (123), (132)\}.$$

(i) Let $H = \{I, (12)\}$. Then H is a subgroup of G. We shall show that H is not a normal subgroup of G.

Take the element $x = (2\ 3)$ of G.

The right coset $Hx = \{I\ (23), (12)(23)\} = \{(23), (132)\}$

and the left coset $xH = \{(23)I, (23)(12)\} = \{(23), (123)\}$.

Since $Hx \neq xH$, therefore H is not a normal subgroup of G.

(ii) Let $H = \{I, (123), (132)\}$ *i.e.*, $H = A_3$, where A_3 is the alternating group of even permutations in S_3. Since $H \neq \{I\}$ and $H \neq G$, therefore H is a non-trivial *i.e.*, a proper subgroup of G.

Also index of H in $G = \frac{o(G)}{o(H)} = \frac{6}{3} = 2$.

Since any subgroup of index two in a group is a normal subgroup of the group, therefore H is a normal subgroup of G.

Problem 8: *H is a normal subgroup of G and K is a subgroup of G such that $H \subseteq K \subseteq G$. Show that H is a normal subgroup of K.* **(Kumaun 2008, 12, 15)**

Solution: H is a normal subgroup of G. Therefore H is a subgroup of G. But K is a subgroup of G and $H \subseteq K$. Therefore H is also a subgroup of K. Now to show that H is normal in K. Let x be any element of K. Then $x \in K \Rightarrow x \in G$. Since H is normal in G, therefore we have $Hx = xH$. Thus H is a subgroup of K and we have $Hx = xH \ \forall \ x \in K$. Hence H is a normal subgroup of K.

Problem 9: *If H is a subgroup of G and N is a normal subgroup of G, show that*

(i) HN is a subgroup of G.

(ii) N is a normal subgroup of HN.

Solution: (i) Proceed as in example 6.

(ii) Since $e \in H$, therefore obviously $N \subseteq HN$. Because if $n \in N$, then we can write $n = en$ which is an element of HN.

Now HN is a subgroup of G and N is also a subgroup of G. Also $N \subseteq HN$. Therefore N is a subgroup of HN. Now to show that N is a normal subgroup of HN. Let $h_1 n_1$ be any element of HN and n be any element of N. Then $h_1 \in H$, $n_1 \in N$ and we have

$$(h_1 n_1)\, n\, (h_1 n_1)^{-1} = h_1 (n_1 n n_1^{-1})\, h_1^{-1} \in N$$

since N is normal in G and $n_1 n n_1^{-1} \in N$, $h_1 \in G$.

Therefore N is a normal subgroup of HN.

Problem 10: *If H is a subgroup of G, let $N(H) = \{ g \in G : gHg^{-1} = H \}$. Show that*

(i) $N(H)$ is a subgroup of G. **(Kumaun 2007, 12)**

(ii) H is a normal subgroup of $N(H)$.

(iii) If H is a normal subgroup of the subgroup K in G, then $K \subseteq N(H)$ i.e., $N(H)$ is the largest subgroup of G in which H is normal.

(iv) H is normal in G if and only if $N(H) = G$.

Solution: Let $a, b \in N(H)$.

Then by def. of $N(H)$, we have $aHa^{-1} = H$ and $bHb^{-1} = H$.

Now $bHb^{-1} = H \Rightarrow b^{-1}(bHb^{-1})b = b^{-1}Hb \Rightarrow H = b^{-1}Hb$.

We have $(ab^{-1})\, H(ab^{-1})^{-1} = ab^{-1}Hba^{-1} = a(b^{-1}Hb)a^{-1}$

$= aHa^{-1}$ $[\because H = b^{-1}Hb]$

$= H$.

$\therefore$ $ab^{-1} \in N(H)$.

Thus $a, b \in N(H) \Rightarrow ab^{-1} \in N(H)$.

Hence $N(H)$ is a subgroup of G.

(ii) Let h be any element of H. Since $h\,H\,h^{-1} = H$, therefore $h \in N(H)$. Thus $H \subseteq N(H)$. Therefore H is a subgroup of $N(H)$. Now to show that H is normal in $N(H)$. Let x be any element of $N(H)$. Then by definition of $N(H)$, we have $x\,H\,x^{-1} = H$. Therefore H is a normal subgroup of $N(H)$.

(iii) Let $k \in K$.

Since H is a normal subgroup of K, therefore we have

$k\,H\,k^{-1} = H \Rightarrow k \in N(H)$. Thus $k \in K \Rightarrow k \in N(H)$. Therefore $K \subseteq N(H)$.

(iv) Let H be normal in G. Let $x \in G$.

Then $x\,H\,x^{-1} = H$ [$\because$ H is normal in G]

$\Rightarrow$ $x \in N(H)$.

Thus $x \in G \Rightarrow x \in N(H)$. Therefore $G \subseteq N(H)$. But $N(H) \subseteq G$.

Therefore $G = N(H)$.

Conversely let $N(H) = G$. Then $x \in G \Rightarrow x \in N(H) \Rightarrow x\,H\,x^{-1} = H$.

Thus we have $x\,H\,x^{-1} = H \ \forall \ x \in G$. Therefore H is a normal subgroup of G.

Problem 11: *Give an example to show that if H is a normal subgroup of G and K is a normal subgroup of H then K may not be a normal subgroup of G.*

Solution: Consider the following subgroups of S_4, the symmetric group of permutations on four symbols a, b, c, d:

$$G = \{I, (abcd), (adcb), (ab)(cd), (ac)(bd), (ad)(bc), (ac), (bd)\},$$

$$H = \{I, (ab)(cd), (ac)(bd), (ad)(bc)\}, \text{ and } K = \{I, (ab)(cd)\}.$$

It can be easily seen that H is a subgroup of G and K is a subgroup of H.

Further any subgroup of index two in a group is a normal subgroup of the group.

Here the index of H in G *i.e.*,

$$[G : H] = o(G)/o(H) = 8/4 = 2.$$

Therefore H is normal in G.

Also $[H : K] = o(H)/o(K) = 4/2 = 2$.

Therefore K is also normal in H.

But here K is not a normal subgroup of G as can be easily seen.

Take the element $(abcd) \in G$ and the element $(ab)(cd) \in K$.

We have $(abcd)(ab)(cd)(abcd)^{-1} = (abcd)(ab)(cd)(dcba) = (ad)(bc) \notin K$.

Therefore K is not a normal subgroup of G.

Comprehensive Problems 2

Problem 1: *(i) Let $f : G \to G'$ be a homomorphism of a group G into a group G'. Prove that $f(G)$ is a sub-group of G' and $f^{-1}(e')$ is a normal sub-group of G, where e' is the identity of G'.* **(Purvanchal 2011)**

(ii) Let R be the additive group of real numbers and U, the multiplicative group of complex numbers of absolute value unity. Prove that the mapping $x \to e^{ix}$ is a homomorphism of R onto U. Find the kernel. **(Meerut 2004)**

Solution: (i) It is given that the mapping f is a homomorphism of a group G into a group G'. We have $f(G) = \{ f(x) : x \in G \}$. Obviously $f(G) \subseteq G'$.

Also $G \neq \varnothing \Rightarrow f(G) \neq \varnothing$.

Let a', b' be any two elements of $f(G)$. Then $f(a) = a', f(b) = b'$ for some $a, b \in G$. We have

$$a'(b')^{-1} = f(a)[f(b)]^{-1} = f(a) f(b^{-1})$$
$$= f(ab)^{-1} \in f(G) \text{ since } ab^{-1} \in G.$$

Thus $a', b' \in f(G) \Rightarrow a'(b')^{-1} \in f(G)$.

Hence $f(G)$ is a subgroup of G'.

Again let $f^{-1}(e') = K$.

Then $K = f^{-1}(e') = \{x \in G : f(x) = e'\}$.

So $K \subseteq G$.

If e is the identity of G, then we know that $f(e) = e'$. So at least $e \in K$ and thus K is not empty.

First we shall show that K is a subgroup of G. Let $a, b \in K$. Then $f(a) = e', f(b) = e'$.

We have $f(ab^{-1}) = f(a) f(b^{-1}) = f(a)[f(b)]^{-1} = e'e'^{-1} = e'e' = e'$.

$\therefore$ $ab^{-1} \in K$, by definition of K.

Thus $k \neq \varnothing$ and $a, b \in K \Rightarrow ab^{-1} \in K$. Therefore K is a subgroup of G. Now to prove that K is normal in G. Let g be any element of G and k be any element of K. Then $f(k) = e'$. We have

$$f(gkg^{-1}) = f(g) f(k) f(g^{-1}) = f(g) e' [f(g)]^{-1}$$
$$= f(g)[f(g)]^{-1} = e'.$$

$\therefore$ $gkg^{-1} \in K$, by definition of K.

Thus $g \in G, k \in K \Rightarrow gkg^{-1} \in K$.

Hence K is a normal subgroup of G and so $f^{-1}(e')$ is a normal subgroup of G.

(ii) Here R is the additive group of real numbers and U is the multiplicative group of complex numbers of absolute value unity.

If x is any real number, then $e^{ix} = \cos x + i \sin x$ is a complex number and

$$|e^{ix}| = |\cos x + i \sin x| = \sqrt{(\cos^2 x + \sin^2 x)} = 1.$$

Thus $\forall\ x \in R$, e^{ix} is a complex number whose modulus is 1.

Let $\phi : R \to U$ be defined as

$$\phi(x) = e^{ix}, \ \forall\ x \in R.$$

The mapping ϕ is onto U: Let $z = x + iy \in U$ *i.e.*, let z be any complex number of unit modulus. Putting z in modulus-argument form, we can write

$$z = 1(\cos\theta + i \sin\theta) = \cos\theta + i \sin\theta, \quad \text{where } \theta \in R.$$

We have $\phi(\theta) = e^{i\theta}$, by definition of mapping ϕ

$$= \cos\theta + i \sin\theta = z.$$

Thus $z \in U \Rightarrow \exists \theta \in R$ such that $\phi(\theta) = z$.

$\therefore$ the mapping ϕ is onto U.

The mapping ϕ is a homomorphism: Let $x_1, x_2 \in R$. Then

$$\phi(x_1 + x_2) = e^{i(x_1 + x_2)} = e^{ix_1}\, e^{ix_2} = \phi(x_1)\,\phi(x_2).$$

$\therefore$ ϕ is a homomorphic mapping.

Hence ϕ is a homomorphism of R onto U.

The identity of the group U is the complex number $1 = 1 + 0i$.

We have $\ker \phi = \{x : x \in R \text{ and } \phi(x) = 1\} = \{x : x \in R \text{ and } e^{ix} = 1\}$.

Now $e^{ix} = 1 \Leftrightarrow \cos x + i \sin x = 1$

$\Leftrightarrow$ $\cos x = 1,\ \sin x = 0$

$\Leftrightarrow$ $x = 2n\pi$ where n is any integer.

$\therefore$ $\ker \phi = \{x : x \in R \text{ and } x = 2n\pi \text{ where } n \text{ an any integer}\}$

$= \{\ldots, -6\pi, -4\pi, -2\pi, 0, 2\pi, 4\pi, 6\pi, \ldots\}$.

Problem 2: *(i) Prove that in a homomorphic mapping of a group G into a group G′, unit element corresponds to unit element, inverses correspond to inverses and subgroups correspond to subgroups.*

(ii) Prove that any quotient group of G is a homomorphic image of G and conversely if G′ is a homomorphic image of G then G′ is isomorphic to a quotient group of G.

Solution: (i) Let f be a homomorphic mapping of a group G into a group G'. Let e and e' be the identity elements of the groups G and G' respectively. Then to prove that

(i) $f(e) = e'$

(ii) $f(a^{-1}) = [f(a)]^{-1}\ \forall\ a \in G$.

For proof see article 10.

Now let H be any subgroup of G. Then to prove that $f(H)$ is a subgroup G'.

We have $f(H) = \{f(x) : x \in H\}$. Obviously $f(H) \subseteq G'$.

Also $H \neq \varnothing \Rightarrow f(H) \neq \varnothing$.

Let a', b' be any two elements of $f(H)$. Then $f(a) = a'$, $f(b) = b'$ for some $a, b \in H$.

We have $a'(b')^{-1} = f(a)[f(b)]^{-1} = f(a)\, f(b^{-1}) = f(ab^{-1}) \in f(H)$,

since $a \in H, b \in H$ and H is a subgroup of $G \Rightarrow ab^{-1} \in H$.

Thus $f(H) \neq \varnothing$ and $a', b' \in f(H) \Rightarrow a'(b')^{-1} \in f(H)$. Hence $f(H)$ is a subgroup of G'.

(ii) Let G be any group and N be a normal subgroup of G. Then G/N is a quotient group of G.

To prove G/N is a homomorphic image of G. We have

$$G/N = \{Nx : x \in G\}.$$

For proof see theorem 4 of article 11.

For the converse part of this question see theorem 5 of article 11.

Problem 3: *G is a group and H is a subgroup of G. Show that the following statements are equivalent :*

(i) *H is a normal subgroup of G.*

(ii) *H is the kernel of a homomorphism of G.*

(iii) *Every left coset of H in G is a right coset of H in G.* **(Avadh 2013)**

Solution: First we shall prove that (i) $\Rightarrow$ (ii).

To prove (i) $\Rightarrow$ (ii).

Let H be a normal subgroup of G. Then to prove that H is the kernel of a homomorphism of G.

Since H is a normal subgroup of G, therefore G/H is a quotient group of G.

We have $G/H = \{Hx : x \in G\}$.

Let $f : G \to G/H$ be defined as

$$f(x) = Hx \quad \forall \quad x \in G.$$

Let Hx be any element of G/H. Then $x \in G$. We have $f(x) = Hx$. Therefore the mapping f is onto G/H.

Let $a, b \in G$. Then

$$f(ab) = Hab = (Ha)(Hb) \qquad [\because H \text{ is a normal subgroup of } G]$$
$$= f(a)\, f(b).$$

$\therefore$ f is a homomorphism of G onto G/H.

Let K be the kernel of this homomorphism f. The identity of the quotient group G/H is the coset H. So $K = \{y \in G : f(y) = H\}$.

We shall prove that $K = H$.

Let $k \in K$. Then $f(k) = H$ *i.e.,* identity of G/H.

But by definition of f, we have $f(k) = Hk$.

Now $Hk = H \Rightarrow k \in H$.

Thus $k \in K \Rightarrow k \in H$.

Therefore $K \subseteq H$.

Again let h be any element of H. Then $Hh = H$.

We have $f(h) = Hh = H$. Therefore $h \in K$.

Thus $h \in H \Rightarrow h \in K$.

$\therefore$ $H \subseteq K$.

Consequently $K = H$.

Hence if H is a normal subgroup of G, then H is the kernel of a homomorphism of G.

$\therefore$ (i) $\Rightarrow$ (ii).

Now to prove (ii) $\Rightarrow$ (i).

Let f be a homomorphism of a group G into a group G' and let H be the kernel of this homomorphism *i.e.*, let

$$H = \{x \in G : f(x) = e', \text{ where } e' \text{ is the identity of } G'\}.$$

Then to prove that H is a normal subgroup of G.

For proof see theorem 1 of article 11.

Hence (ii) $\Rightarrow$ (i).

Thus (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (i). Therefore the statements (i) and (ii) are equivalent.

Now we shall prove that (i) $\Rightarrow$ (iii) *i.e.*, (i) $\Rightarrow$ (iii) and (iii) $\Rightarrow$ (i).

For proof see theorem 2 of article 1 of this chapter. Thus the statements (i) and (iii) are equivalent. Hence the given statements (i), (ii) and (iii) are equivalent.

Problem 4: *(i) Show that two elements are conjugate if and only if they can be put in the form xy and yx respectively where x and y are suitable elements of G.*

(ii) Let N_1 and N_2 be two normal subgroups of a group G. Prove that $G/N_1 = G/N_2$ if and only if $N_1 = N_2$.

(iii) Give an example to show that in a group G the normalizer of an element is not necessarily a normal subgroup of G.

Solution: (i) Let a, b be two conjugate elements of a group G.

Then $a = c^{-1} b c$ for some $c \in G$.

Let $c^{-1} b = x$ and $c = y$. Then $a = xy$.

Also $y x = c (c^{-1} b) = (c c^{-1}) b = e b = b$.

Conversely suppose that $a = x y$ and $b = y x$. We have

$$b = y x \Rightarrow y^{-1} b = y^{-1} y x \Rightarrow y^{-1} b = x .$$

Now $a = x y \Rightarrow a = y^{-1} by \Rightarrow a$ and b are conjugate elements.

(ii) If $N_1 = N_2$, then obviously $G/N_1 = G/N_2$.

Conversely suppose that $G/N_1 = G/N_2$. Then we are to prove that $N_1 = N_2$. We have $N_1 \in G/N_1$. But $G/N_1 = G/N_2$. Therefore $N_1 \in G/N_2$ *i.e.*, N_1 is equal to some coset of N_2 in G. But two cosets of N_2 in G are either disjoint or identical. Since $e \in N_1$ and $e \in N_2$, therefore N_1 and N_2 are not disjoint. So we must have $N_1 = N_2$.

(iii) Consider the group S_3, the symmetric group of permutations on three symbols a, b, c. We have $S_3 = \{I, (ab), (bc), (ca), (abc), (acb)\}$. Let $N(ab)$ denote the normalizer of the element $(ab) \in S_3$. We shall show that $N(ab)$ is not a normal subgroup of S_3. Let us calculate the elements of $N(ab)$. Obviously $(ab) \in N(ab)$. Also $I \in N(ab)$ because $I(ab) = (ab) I$.

Now $(bc)(ab) = (abc)$ and $(ab)(bc) = (acb)$. Thus (bc) does not commute with (ab). Therefore $(bc) \notin N(ab)$.

Again $(ca)(ab) \neq (acb)$ and $(ab)(ca) = (abc)$.

Thus $(ca)(ab) \neq (ab)(ca)$ and therefore $(ca) \notin N(ab)$. Similarly we can verify that

$(abc) \notin N(ab)$ and $(acb) \notin N(ab)$.

Hence $N(ab) = \{ I, (ab) \}$.

Now we shall show that $N(ab)$ is not a normal subgroup of S_3. Take the element $(bc) \in S_3$ and the element $(ab) \in N(ab)$. We have

$$(bc)(ab)(bc)^{-1} = (bc)(ab)(cb) = (abc)(cb) = (ac) \notin N(ab).$$

Therefore $N(ab)$ is not a normal subgroup of S_3.

Problem 5: *(i) Prove that every normal subgroup of a group G gives rise to a homomorphism from G. Moreover, show that with every homomorphism from G we can associate a unique normal subgroup of G.*

(ii) If ϕ be a homomorphism of a group G onto the group $\overline{G}$ with kernel K, then prove that the set of all inverse images of $\bar{g} \in \overline{G}$ under ϕ in G is given by Kx where x is any particular inverse image of $\bar{g}$ in G. **(Kashi 2011)**

(iii) Write down the elements of the symmetric group P_3 and determine the classes of conjugate elements.

Solution: (i) Let G be a group and N be a normal subgroup of G. Then G/N is a quotient group of G.

We have $G/N = \{Nx : x \in G\}$.

Let $f : G \to G/N$ be defined as

$f(x) = Nx \quad \forall \quad x \in G$.

We shall show that f is a homomorphism of G onto G/N.

For proof see theorem 4 of article 11.

Hence every normal subgroup of a group G gives rise to a homomorphism from G.

Second part of the question: Let f be a homomorphism of a group G into a group G'.

Then we are to show that we can associate with f a unique normal subgroup of G.

Let e, e' be the identities of G and G' respectively. Let

$$K = \text{kernel } f = \{x \in G : f(x) = e'\}.$$

Then K is a normal subgroup of G. For proof see theorem 1 of article 11.

Thus we have associated with f a normal subgroup K of G. Since kernel f is unique, therefore the normal subgroup K of G associated with f is unique.

(ii) Let ϕ be a homomorphism of a group G onto the group $\overline{G}$ with kernel K and let e, e' be the identities of G and $\overline{G}$ respectively.

Let $\bar{g} \in \overline{G}$ and let x be any particular inverse image of $\bar{g}$ in G under the mapping ϕ *i.e.*, $x \in G$ and $\phi(x) = \bar{g}$.

We have $\phi^{-1}(\bar{g})$ = the set of all inverse images of $\bar{g}$ in G under ϕ

$$= \{y \in G : \phi(y) = \bar{g}\}.$$

To prove that $\phi^{-1}(\bar{g}) = Kx$.

Let $u \in Kx$. Then $u = kx$ for some $k \in K$.

We have $\phi(u) = \phi(kx) = \phi(k)\,\phi(x)$

$= e'\,\phi(x)$ $\qquad [\because \ k \in K \Rightarrow \phi(k) = e']$

$= \phi(x) = \bar{g}$.

$\therefore \quad u \in \phi^{-1}(\bar{g})$.

Thus $u \in Kx \Rightarrow u \in \phi^{-1}(\bar{g})$.

$\therefore \quad Kx \subseteq \phi^{-1}(\bar{g})$. ...(1)

Now let z be any element of $\phi^{-1}(\bar{g})$. Then $\phi(z) = \bar{g}$.

We have $\phi(zx^{-1}) = \phi(z)\,\phi(x^{-1}) = \phi(z)\,[\phi(x)]^{-1}$

$= g - (g-)^{-1} = e'.$

$\therefore \quad z\,x^{-1} \in K \Rightarrow (z\,x^{-1})\,x \in K\,x \Rightarrow z \in K\,x.$

Thus $z \in \phi^{-1}(\bar{g}) \Rightarrow z \in K\,x.$

$\therefore \quad \phi^{-1}(\bar{g}) \subseteq K\,x.$ ...(2)

From (1) and (2), we get $\phi^{-1}(\bar{g}) = K\,x.$

(iii) Let P_3 be the symmetric group of permutations on three symbols 1, 2, 3.

We have $P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$,

where f_1 = identity permutation I,

$f_2 = (12), \quad f_3 = (23), \quad f_4 = (31), \quad f_5 = (123)$

and $f_6 = (132).$

Now in a group G the conjugate class $C(a)$ of a in G is defined as

$C(a) = \{x \in G : x \sim a\}$

and we have $C(a) = \{y^{-1}ay : y \in G\}.$

$\therefore \quad C(f_1) = \{f_1^{-1} f_1 f_1,\ f_2^{-1} f_1 f_2,\ f_3^{-1} f_1 f_3,\ f_4^{-1} f_1 f_4,$

$f_5^{-1} f_1 f_5,\ f_6^{-1} f_1 f_6\}$

$= \{f_1\},$

$C(f_2) = \{I^{-1}(12)I,\ (12)^{-1}(12)(12), (23)^{-1}(12)(23),$

$(31)^{-1}(12)(31),\ (123)^{-1}(12)(123),\ (132)^{-1}(12)(132)\}$

$= \{(12),\ (12)(12)(12),\ (23)(12)(23),\ (31)(12)(31),$

$(321)(12)(123),\ (231)(12)(132)\}$

$= \{(12), (12), (13), (23), (23), (13)\}$

$= \{(12), (23), (31)\}$

$= \{f_2, f_3, f_4\}.$

Since $f_3 \sim f_2$ and $f_4 \sim f_2$, therefore

$C(f_3) = C(f_2)$ and $C(f_4) = C(f_2).$

$\therefore \quad C(f_3) = \{f_2, f_3, f_4\}$

and $C(f_4) = \{f_2, f_3, f_4\}.$

Again $C(f_5) = \{I^{-1}(123)I, (12)^{-1}(123)(12), (23)^{-1}(123)(23),$

$(31)^{-1}(123)(31), (123)^{-1}(123)(123), (132)^{-1}(123)(132)\}$

$= \{(123), (12)(123)(12), (23)(123)(23), (31)(123)(31),$

$(321)(123)(123), (231)(123)(132)\}$

$= \{(123), (132), (132), (321), (123), (123)\}$

$= \{(123), (132)\} = \{f_5, f_6\}.$

Since $f_6 \sim f_5$, therefore

$C(f_6) = C(f_5) = \{f_5, f_6\}.$

Hence $C(f_1) = \{f_1\}$,
$C(f_2) = C(f_3) = C(f_4) = \{f_2, f_3, f_4\}$
and $C(f_5) = C(f_6) = \{f_5, f_6\}$.

Problem 6: *(i) Show that any two conjugate classes of a group are either disjoint or identical.*
(ii) If N is a normal subgroup of a group G, having the prime index p, prove that G/N is cyclic.

Solution: If a, b be two elements of a group G, then b is said to be conjugate to a if there exists an element $x \in G$ such that

$$b = x^{-1} ax.$$

Also then symbolically we write $b \sim a$.
We know that the relation of conjugacy is an equivalence relation on G *i.e.*, it is reflexive, symmetric and transitive.
If $a \in G$, then the conjugate class $C(a)$ of a in G is defined as

$$C(a) = \{x \in G : x \sim a\}.$$

First we shall show that if $a \sim b$, then $C(a) = C(b)$.
Let $a \sim b$.
We have $x \in C(a) \Rightarrow x \sim a$. But $a \sim b$.
$\therefore$ $x \sim a$ and $a\,0 \sim b \Rightarrow x \sim b$
[$\because$ the relation $\sim$ on G is transitive]
$\Rightarrow$ $x \in C(b)$.
Thus $x \in C(a) \Rightarrow x \in C(b)$.
$\therefore$ $C(a) \subseteq C(b)$ ...(1)
Again $y \in C(b) \Rightarrow y \sim b$. But $a \sim b$.
$\therefore$ $b \sim a$ because the relation $\sim$ on G is symmetric.
$\therefore$ $y \sim b$ and $b \sim a \Rightarrow y \sim a$
$\Rightarrow$ $y \in C(a)$.
Thus $y \in C(b) \Rightarrow y \in C(a)$.
$\therefore$ $C(b) \subseteq C(a)$. ...(2)
From (1) and (2) we conclude that $C(a) = C(b)$.
Hence if $a \sim b$, then we have $C(a) = C(b)$.
Now let $C(a)$ and $C(b)$ be two conjugate classes in G. We are to prove that either $C(a)$ and $C(b)$ are disjoint or they are identical.
If $C(a) \cap C(b) = \varnothing$, the proof is complete because then $C(a)$ and $C(b)$ are disjoint.
So let $C(a) \cap C(b) \neq \varnothing$.
Then to prove that $C(a) = C(b)$.
Since $C(a) \cap C(b) \neq \varnothing$, therefore let $x \in C(a) \cap C(b)$.
Then $x \in C(a)$ and $x \in C(b)$.
We have $x \in C(a) \Rightarrow x \sim a$
and $x \in C(b) \Rightarrow x \sim b$.

Now $x \sim a \Rightarrow a \sim x$.

Also $a \sim x$ and $x \sim b \Rightarrow a \sim b$.

But $a \sim b \Rightarrow C(a) = C(b)$.

Hence if $C(a) \cap C(b) \neq \varnothing$, then we have $C(a) = C(b)$.

Therefore any two conjugate classes of a group are either disjoint or identical.

(ii) Let G be a group and N be a normal subgroup of G so that G/N is a quotient group of G.

It is given that the index of N in G is a prime number p.

We have $G/N = \{Nx : x \in G\}$.

$\therefore$ $o(G/N)$ = The number of distinct right cosets of N in G

= the index of N in G

= p, where p is a prime number.

Now we know that every group of prime order is cyclic. Hence G/N is cyclic.

Problem 7: *(i) Show that every homomorphic image of an abelian group is abelian and the converse is not true.*

(ii) Show that a homomorphism from a simple group is either trivial or one-to-one.

Solution: (i) Let G be an abelian group. Let f be a homomorphic mapping of G onto a group G'. Then G' is a homomorphic image of G.

Let a', b' be any two elements of G'. Then $f(a) = a'$, $f(b) = b'$ for some $a, b \in G$.

We have

$$a'b' = f(a)\, f(b) = f(ab) = f(ba) \qquad [\because G \text{ is abelian}]$$
$$= f(b)\, f(a) = b'a'.$$

$\therefore$ G' is abelian.

The converse is not true. P_3 is a non-abelian group. A_3 is a normal subgroup of P_3. The quotient group P_3 / A_3 is a homomorphic image of P_3. Now P_3 / A_3 is of order 2 and is abelian.

(ii) Let G be a simple group and f be a homomorphism of G into another group G'. Then ker f is a normal subgroup of G. But the only normal subgroups of the simple group G are G itself and $\{e\}$. Therefore either ker $f = G$ or ker $f = \{e\}$. If ker $f = G$, the f-image of each element of G is the identity of G' and so the homomorphism f is a trivial one. If ker $f = \{e\}$, the homomorphism f is one-to-one. Hence the result.

Problem 8: *Let $(G, +)$ be an abelian group. Let S be the set of all endomorphisms of G. For any $\sigma, \eta \in S$ define $\sigma + \eta : G \to G$ by $(\sigma + \eta)(x) = \sigma(x) + \eta(x)$.*

Show that $\sigma + \eta$ is also an endomorphism of G. Further show that S becomes an abelian group with respect to this addition composition.

Solution: G is an additive abelian group and $S = \{ f : f \text{ is an endomorphism of } G \}$. If $\sigma, \eta \in S$, we have defined $\sigma + \eta$ as follows :

$$(\sigma + \eta)(x) = \sigma(x) + \eta(x) \quad \text{for all} \quad x \in G.$$

Since $\sigma(x), \eta(x) \in G \Rightarrow \sigma(x) + \eta(x) \in G$, therefore $\sigma + \eta$ is a mapping of G into itself. We shall show that $\sigma + \eta$ is also an endomorphism of G *i.e.*, $\sigma + \eta$ is a homomorphism of G into G. For all $a, b \in G$, we have

$$(\sigma + \eta)(a + b) = \sigma(a + b) + \eta(a + b) \qquad \text{[By def. of } \sigma + \eta\text{]}$$
$$= [\sigma(a) + \sigma(b)] + [\eta(a) + \eta(b)] \qquad [\because \sigma \text{ and } \eta \text{ are endomorphisms}]$$
$$= [\sigma(a) + \eta(a)] + [\sigma(b) + \eta(b)] \qquad [\because G \text{ is an abelian group}]$$
$$= (\sigma + \eta)(a) + (\sigma + \eta)(b). \qquad \text{[By def. of } \sigma + \eta \text{]}$$

Therefore $\sigma + \eta$ is an endomorphism of G. Thus $\sigma \in S, \eta \in S \Rightarrow \sigma + \eta \in S$. Therefore S is closed with respect to the addition defined on it. Now we shall show that S is an abelian group with respect to the addition defined on it.

Associativity of addition on *S*: For all $f, g, h \in S$ and for all $x \in G$, we have

$$[(f + g) + h](x) = (f + g)(x) + h(x) \qquad \text{[By def. of addition of } S\text{]}$$
$$= [f(x) + g(x)] + h(x) \qquad \text{[By def. of addition of } S\text{]}$$
$$= f(x) + [g(x) + h(x)] \qquad \text{[By associativity in G]}$$
$$= f(x) + (g + h)(x) = [f + (g + h)](x).$$

Therefore by definition of equality of two functions, we have

$$(f + g) + h = f + (g + h).$$

Thus addition defined on S is associative.

Commutativity of addition on *S*: For all $x \in G$, we have

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

Therefore $f + g = g + f$.

Existence of additive identity in *S*: Let 0 denote the identity element of the group G. Let us define a mapping $\hat{0}$ of G into itself by the rule $\hat{0}(x) = 0, \forall\ x \in G$.

For all $a, b \in G$, we have

$$\hat{0}(a + b) = 0 = 0 + 0 = \hat{0}(a) + \hat{0}(b).$$

Therefore $\hat{0}$ is an endomorphism of G *i.e.*, $\hat{0} \in S$.

Now for all $f \in S$ and for all $x \in G$, we have

$$(\hat{0} + f)(x) = \hat{0}(x) + f(x) = 0 + f(x) = f(x).$$

Therefore $\hat{0} + f = f$, by def. of equality of two mappings

$= f + \hat{0}$, since addition on S is commutative.

Thus $\hat{0} \in S$ is the additive identity.

Existence of the additive inverse of each element of *S*: Let $f \in S$. Let us define a mapping

$-f$ of G into itself by the rule

$$(-f)(x) = -f(x), \forall\ x \in G.$$

For all $a, b \in G$, we have

$$(-f)(a+b) = -f(a+b) = -[f(a) + f(b)]$$
$$= [-f(a)] + [-f(b)] = (-f)(a) + (-f)(b).$$

Therefore $-f$ is an endomorphism of G.

Now for all $x \in G$, we have

$$(-f+f)(x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = \hat{0}(x).$$

Therefore $\quad -f + f = \hat{0}.$

Thus $-f \in S$ is the additive inverse of $f \in S$.

Hence S is an abelian group with respect to the addition composition defined on it.

Problem 9: *(i) Show that it is impossible to find a homomorphism of Z onto S_n $(n > 2)$. Here Z is the additive group of integers.*

(ii) State and prove fundamental theorem of homomorphism for groups. Deduce that if a group G' is a homomorphic image of a finite group G, the order of G' divides the order of G.

Solution: (i) Z is the additive group of integers and S_n is the symmetric group of permutations of degree n.

Let, if possible, f be a homomorphism of Z onto S_n $(n > 2)$. Let $K = \ker f$.

Then by fundamental theorem on homomorphism of groups, we have

$$Z/K \cong S_n.$$

Now Z is an abelian group and every quotient group of an abelian group is abelian. So the quotient group Z/K of the group Z is abelian. But if $n > 2$, then S_n is non-abelian. Since every isomorphic image of an abelian group is abelian, therefore the abelian group Z/K cannot be isomorphic to the non-abelian group S_n.

So our initial assumption that f is a homomorphism of Z onto S_n $(n > 2)$ is wrong. Hence it is impossible to find a homomorphism of Z onto S_n $(n > 2)$.

(ii) For the first part of this question see theorem 5 of article 11.

Second part of the question.

Let G be a finite group and G' be the homomorphic image of G and f be the corresponding homomorphism.

Let $\ker f = K$.

Then by fundamental theorem on homomorphism of groups, we have

$$G/K \cong G'.$$

$\therefore \quad o(G') = o(G/K)$

$$= \text{the number of distinct right cosets of } K \text{ in } G$$

$$= \frac{o(G)}{o(K)}, \text{ by Lagrange's theorem.}$$

$\therefore \quad o(G').\, o(K) = o(G)$

$\Rightarrow \quad \dfrac{o(G)}{o(G')} = o(K)$

$\Rightarrow \quad o(G')$ is a divisor of $o(G)$.

Problem 10: *(i) How many homomorphisms are there from Z_6 onto Z_5 ? Here Z_n denotes the additive group of residue classes modulo n.*

(ii) If the order of a group G is a power of a prime p, show that the centre of G has at least p elements.

Solution: (i) The order of the group Z_6 is 6 and $o(Z_5) = 5$.

Let, if possible, f be a homomorphism of Z_6 onto Z_5 . Let $K = \ker f$.

Then by fundamental theorem on homomorphism of groups, we have

$$Z_6 / K \cong Z_5 .$$

Now K is a subgroup of a finite group Z_6. By Lagrange's theorem $o(K)$ is a divisor of $o(Z_6)$ which is 6. So we can have $o(K) = 1, 2, 3$ or 6.

If $o(K) = 1$, then $o(Z_6 / K) = \dfrac{o(Z_6)}{o(K)} = \dfrac{6}{1} = 6$

while $o(Z_5)$ is 5. So we cannot have $Z_6 / K \cong Z_5$. (Note that two finite groups G and H of different orders can never be isomorphic.)

If $o(K) = 2$, then $o(Z_6 / K) = \dfrac{o(Z_6)}{o(K)} = \dfrac{6}{2} = 3$ and so we cannot have $Z_6 / K \cong Z_5$.

Again if $o(K) = 3$, then $o(Z_6 / K) = 6/3 = 2$ and so we cannot have $Z_6 / K \cong Z_5$.

Finally if $o(K) = 6$, then $o(Z_6 / K) = 6/6 = 1$ and so we cannot have $Z_6 / K \cong Z_5$.

Thus in all cases we cannot have $Z_6 / K \cong Z_5$.

So our initial assumption that f is a homomorphism of Z_6 onto Z_5 is wrong. Hence there is no homomorphism of Z_6 onto Z_5 .

(ii) Let $o(G) = p^n$, where p is prime and n is some positive integer.

Let Z be the centre of G.

Since $o(G) = p^n$, therefore $Z \neq \{e\}$. [See theorem 4 of article 5]

Thus Z contains some elements of G other than e also.

$\therefore \quad o(Z) > 1$.

By Lagrange's theorem $o(Z)$ is a divisor of $o(G)$.

Since $o(G) = p^n$, where p is prime,

therefore $o(Z) = p^m$, where m is an integer such that $1 \leq m \leq n$.

$\therefore$ Z contains at least p elements.

Comprehensive Problems 3

Problem 1: *Let G be a finite abelian additive group and n be a positive integer relatively prime to $o(G)$. Prove that the mapping $\sigma : G \to G$ given by $\sigma(x) = nx$ is an automorphism of G.*

Solution: **The mapping σ is one-one:** Let x, y be any two elements of G. Then

$$\sigma(x) = \sigma(y) \Rightarrow nx = ny$$

$$\Rightarrow \quad n(x - y) = 0 \text{ , where 0 is the identity of the group } G$$

$\Rightarrow$ $o(x-y) \mid n$

$\Rightarrow$ $o(x-y) \mid n$ and $o(x-y) \mid o(G)$ $[\because o(x-y) \mid o(G)]$

$\Rightarrow$ $o(x-y) = 1$ $[\because$ if $o(x-y) \neq 1$, then $o(x-y) > 1 \Rightarrow n$ and $o(G)$ are not relatively prime$]$

$\Rightarrow$ $x - y = o$ *i.e.,* the identity of G

$\Rightarrow$ $x = y$.

Therefore the mapping σ is one-one.

The mapping σ is also onto G: Since G is finite and σ is one-one, therefore σ must be onto G.

Finally if $x, y \in G$, then $\sigma(x+y) = n(x+y) = nx + ny = \sigma(x) + \sigma(y)$.

Hence, σ is an automorphism of G.

Problem 2: *Verify the following statement for being true or false :*

If $G = (a)$ is a cyclic group of order 10 then the mapping $\sigma : G \to G$ such that $\sigma(a^k) = a^{2k}$ for all k, is an automorphism of G.

Solution: The given statement is false as shown below.

Let $G = \{a, a^2, a^3, a^4, \ldots, a^{10} = e\}$.

The mapping σ is not one-one as shown below.

Obviously a^5 and $a^{10} = e$ are two distinct elements of G.

We have $\sigma(a^5) = (a^5)^2 = a^{10} = e$

and $\sigma(a^{10}) = (a^{10})^2 = e^2 = e$.

Thus $\sigma(a^5) = \sigma(a^{10})$ though $a^5 \neq a^{10}$.

$\therefore$ the mapping σ is not one-one.

Hence, σ is not an automorphism of G.

Problem 3: *Give an example of a group in which (i) the inner automorphisms corresponding to any two elements are the same, (ii) the inner automorphisms corresponding to no two elements are the same.*

Solution: (i) Let G be any abelian group.

We know that for an abelian group the only inner automorphism is the identity mapping. Hence, the inner automorphisms corresponding to any two elements of G are the same.

(ii) Let P_3 be the symmetric group of permutations of degree 3 on the set

$S = \{1, 2, 3\}$.

Let $P_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$,

where f_1 = identity permutation,

$f_2 = (1\,2)$, $f_3 = (2\,3)$, $f_4 = (3\,1)$, $f_5 = (1\,2\,3)$ and $f_6 = (1\,3\,2)$.

It can be shown that the inner automorphisms corresponding to no two elements of P_3 are the same.

Let us find the inner automorphisms corresponding to $f_1, f_2, \ldots, f_6$.

The inner automorphism corresponding to f_1 is the identity mapping of P_3 *i.e.*, is given by

$$\begin{matrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \end{matrix}.$$

Now we find the inner automorphism corresponding to f_2. It is given as below.

$$\begin{matrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_2^{-1} f_1 f_2 & f_2^{-1} f_2 f_2 & f_2^{-1} f_3 f_2 & f_2^{-1} f_4 f_2 & f_2^{-1} f_5 f_2 & f_2^{-1} f_6 f_2 \end{matrix}$$

i.e., by

$$\begin{matrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_1 & f_2 & f_4 & f_3 & f_6 & f_5 \end{matrix}$$

$[\because\ f_2^{-1} f_3 f_2 = (12)^{-1}(23)(12) = (12)(23)(12) = (1\,3) = (31) = f_4\ ;$

$f_2^{-1} f_4 f_2 = (12)(31)(12) = (2\,3) = f_3\ ;\ f_2^{-1} f_5 f_2 = (12)(123)(12) = (1\,3\,2) = f_6\ ;$

$f_2^{-1} f_5 f_2 = (12)(132)(12) = (123) = f_5\ ]$

Similarly we find the inner automorphisms corresponding to f_3, f_4, f_5 and f_6.
We can see that the inner automorphisms corresponding to no two elements of P_3 are the same.

Problem 4: *Show that the group of all automorphisms of a cyclic group G of order r is isomorphic to the group of integers less than and relatively prime to r under multiplication modulo r.*

Solution: See article 16.

Hints to Objective Type Questions

Multiple Choice Questions

1. See article 1, Theorem 2.
2. See article 9.
3. See Example 14.
4. See Example 28.
5. See Example 26.
6. See Example 21.
7. See article 11, Theorem 5. Fundamental theorem on homomorphism of groups.
8. See Problem 7(i) of Comprehensive Problems 2.
9. See Example 25.
10. See article 1, Theorem 3.
11. See Example 8.
12. See article 5, Theorem 4.

13. See article 9, Theorem. Existence of identity.
14. See Problem 4(ii) of Comprehensive Problems 2.
15. See article 1. Definition of a simple group.

Fill in the Blank(s)

1. See article 1. Definition of a simple group.
2. See Example 1.
3. See Example 4.
4. See article 5, the definition of the centre of a group.
5. See article 1, Theorem 2.
6. See article 3, the definition of normalizer of an element of a group.
7. See article 9, the definition of a quotient group.
8. See article 11. Definition of Kernel of a Homomorphism.
9. See article 11, Theorem 3.
10. See article 11, Theorem 5. Fundamental theorem on homomorphism of group.
11. See article 10, Definition of Endomorphism.
12. See Problem 7(i) of Comprehensive Problems 2.

True or False

1. See article 1, Theorem 4.
2. See Example 1.
3. See Example 3.
4. If N is a normal subgroup of G, then we have
   $$(Na)(Nb) = Nab, \quad \forall \ a, b \in G.$$
   See article 9.
5. See article 2, Theorem 1.
6. See Note 1 after article 3, Theorem 1.
   Also refer Problem 4 (iii) of Comprehensive Problems 2.
7. See article 5, Theorem 4.
8. We know that every group of order p^2 is abelian,
   where p is a prime number. We have $121 = 11^2$, where 11 is prime.
   Hence, every group of order 121 is abelian.
9. Here, K is a normal subgroup of G.
   See article 11, Theorem 1.
10. See Problem 7(ii) of Comprehensive Problems 2.
11. See Example 9.

○○○

Chapter-9

Rings

Comprehensive Problems 1

Problem 1: *Prove that the set of rational numbers (real numbers or complex numbers) is a field with respect to addition and multiplication.*

Solution: We shall give proof in the case of the set of rational numbers and a similar proof can be given in the case of the set of real numbers or the set of complex numbers.

Let **Q** denote the set of rational numbers. Remember that a rational number is of the form a / b, where a and b are integers and $b \neq 0$.

To prove that the algebraic structure $(\mathbf{Q}, +, \bullet)$ is a field.

$(\mathbf{Q}, +)$ is an abelian group: We know that the sum of two rational numbers is also a rational number. Therefore **Q** is closed for addition of rational numbers.

Also addition of rational numbers is commutative as well as associative. The rational number 0 is identity for addition of rational numbers. Also if a / b is any rational number, then the rational number $-a / b$ is its additive inverse. Thus $(\mathbf{Q}, +)$ is an abelian group.

Now the product of two rational numbers is also a rational number. Therefore **Q** is closed for multiplication of rational numbers.

Also multiplication of rational numbers is commutative as well as associative and it distributes over addition of rational numbers. The rational number 1 is identity for multiplication. Thus $(\mathbf{Q}, +, \bullet)$ is a commutative ring with unity 1.

If a / b is any non-zero rational number, then the integer $a \neq 0$ and so b / a is also a rational number.

We have $(a / b)(b / a) = 1$, so that b / a is the multiplicative inverse of a / b. Thus each non-zero rational number possesses multiplicative inverse. Hence $(\mathbf{Q}, +, \bullet)$ is a field.

Note: To give the proof in the case of the set of complex numbers denote the set of the complex numbers by **C.**

Remember that a complex number is of the form $a + ib$ where a and b are any real numbers.

If $a + ib$ and $c + id$ are any two complex numbers, then

$(a + ib) + (c + id) = (a + c) + i(b + d)$ which is also a complex number.

and $(a + ib)(c + id) = (ac - bd) + i(ad + bc)$ which is also a complex number.

The complex number 0 *i.e.*, $0 + i0$ is identity for addition of complex numbers. Also if $a + ib$ is any complex number, then the complex number $-a - ib$ *i.e.*, $(-a) + i(-b)$ is its additive inverse.

The complex number 1 *i.e.*, $1 + i0$ is identity for multiplication.

Finally every non-zero complex number possesses multiplicative inverse as shown below.

Let $a + ib$ be any non-zero complex number *i.e.*, $a + ib \neq 0 + i0$. Then a and b are real numbers and at least one of them is not zero.

Suppose the complex number $x + iy$ is the multiplicative inverse of $a + ib$. Then

$$(x + iy)(a + ib) = 1 + i0$$

$$\Rightarrow \quad (xa - yb) + i(xb + ya) = 1 + i0$$

$$\Rightarrow \quad xa - yb = 1, xb + ya = 0.$$

Solving the equations $xa - yb = 1, xb + ya = 0$, we get

$$x = \frac{a}{a^2 + b^2}, y = \frac{-b}{a^2 + b^2}.$$

Since at least one of a and b is not zero, therefore the real number $a^2 + b^2 \neq 0$ and so both x and y are some real numbers.

Therefore the complex number $\frac{a}{a^2 + b^2} + i\left(\frac{-b}{a^2 + b^2}\right)$ is the multiplicative inverse of the non-zero complex number $a + ib$.

Problem 2: *(i) Prove that the set of integers is an integral domain with respect to addition and multiplication.*

(ii) Define a field. Prove that every field is an integral domain, but there exist some integral domains which are not fields.

Solution: (i) Let $\mathbf{I} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ be the set of integers. To prove that the algebraic structure $(\mathbf{I}, +, \bullet)$ is an integral domain.

$(\mathbf{I}, +)$ is an abelian group: We know that the sum of two integers is also an integer. Therefore $\mathbf{I}$ is closed for addition of integers.

Also addition of integers is commutative as well as associative. The integer 0 is identity for addition of integers. Also if a is any integer in $\mathbf{I}$, then the integer $-a$ is its additive inverse.

Thus $(\mathbf{I}, +)$ is an abelian group.

Now the product of two integers is also an integer. Therefore $\mathbf{I}$ is closed for multiplication of integers.

Also multiplication of integers is associative as well as commutative and it distributes over addition of integers. The integer 1 is identity for multiplication. Further the product of two integers can be zero only if at least one of them is zero.

Hence the algebraic structure $(\mathbf{I}, +, \bullet)$ is a commutative ring with unity and without zero divisors and so it is an integral domain.

(ii) For the definition of a field refer article 7. To prove that every field is an integral domain refer theorem 1 of article 8.

For an example of a ring which is an integral domain but is not a field, consider the ring of integers $(\mathbf{I}, +, \bullet)$ where $\mathbf{I}$ is the set of integers *i.e.*,

$$\mathbf{I} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

The ring of integers $(\mathbf{I}, +, \bullet)$ is an integral domain because it is a commutative ring with unity 1 and does not possess zero divisors. But this ring is not a field.

The only elements of the ring of integers which possess multiplicative inverse are 1 and -1 while in a field every non-zero element must possess multiplicative inverse.

Hence the ring of integers is an integral domain but it is not a field.

Problem 3: *Define a ring and furnish an example of (i) a non-commutative ring with unity, (ii) a commutative ring without unity.* **(Kumaun 2008, 10)**

Solution: For the definition of a ring refer article 1.

(i) Example of a non-commutative ring with unity:

Let M be the set of all 2×2 matrices with elements as real numbers. Then M is a ring for addition and multiplication of matrices as the two ring operations.

This ring is a non-commutative ring because the operation of multiplication of matrices on the set M is not commutative. For example, if we take $A = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}, B = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ as two members of M, we find that

$$AB = \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 8 \\ 3 & 11 \end{bmatrix}$$

and $$BA = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 8 & 14 \\ 3 & 5 \end{bmatrix}.$$

Thus $AB \neq BA$ and so the ring is a non-commutative ring.
But this ring is a ring with unity.

The unit matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M$ and is identity for multiplication of matrices because we have $IA = A = AI \ \forall A \in M$.

Therefore the unit matrix I is the unity element of this ring.

Hence the ring of 2×2 matrices with elements as real numbers is a non-commutative ring with unity.

(ii) Example of a commutative ring without unity: The ring of even integers $(2\mathbf{I}, +, \bullet)$, *i.e.*, the ring $(\{..., -6, -4, -2, 0, 2, 4, 6, ...\}, +, \bullet)$ is a commutative ring without unity.

Since the multiplication of integers is a commutative operation, therefore the ring of even integers is a commutative ring. But this ring is without unity because it does not possess multiplicative identity. In the set of even integers there exists no even integer e such that $ea = a = ae, \forall a \in 2\mathbf{I}$.

Hence $(2\mathbf{I}, +, \bullet)$ is a commutative ring without unity.

Problem 4 : *(i) Prove that in the list of axioms for a ring R with unity the axiom demanding commutativity under addition may be omitted.*

(ii) If R is a system satisfying all the conditions for a ring with unit element with the possible exception $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

(iii) Let C be the set of the ordered pairs (a, b) of real numbers. Define addition and multiplication in C by the equations

$$(a, b) + (c, d) = (a + c, b + d), \ (a, b)(c, d) = (ac - bd, bc + ad).$$

Prove that $\mathbf{C}$ *is a field.*

Solution: (i) Suppose an algebraic structure $(R, +, \bullet)$ satisfies all the axioms for a ring with unity except the axiom of commutativity of addition. Then we have to show that addition must be commutative on R and thus R must be a ring.

Now proceed as in part (ii).

(ii) Since 1 is an element of R, we have

$$(a + b)(1 + 1) = a(1 + 1) + b(1 + 1) \quad \text{[By right distributive law]}$$
$$= (a1 + a1) + (b1 + b1) = (a + a) + (b + b) \quad \ldots(1)$$

Also $$(a + b)(1 + 1) = (a + b)1 + (a + b)1 \quad \text{[By left distributive law]}$$
$$= (a + b) + (a + b) \quad \ldots(2)$$
$$[\because 1 \text{ is the unit element}]$$

From (1) and (2), we get

$$(a + a) + (b + b) = (a + b) + (a + b)$$
$$\Rightarrow \quad [(a + a) + b] + b = [(a + b) + a] + b \quad \text{[By associativity of addition]}$$
$$\Rightarrow \quad (a + a) + b = (a + b) + a \quad \text{[By right cancellation law for addition in } R \text{ since with the given postulates } R \text{ is a group with respect to addition]}$$
$$\Rightarrow \quad a + (a + b) = a + (b + a) \quad \text{[By associativity of addition in } R \text{]}$$
$$\Rightarrow \quad (a + b) = (b + a) \quad \text{[By left cancellation law for addition in } R \text{]}$$

Thus addition is commutative in R. Hence R is a ring.

(iii) **Proof:** We see that **C** is closed with respect to the two compositions since

$$a + c, b + d, ac - bd, bc + ad$$

are all real numbers. Now let $(a, b), (c, d), (e, f)$ be any elements of **C**. Then we make the following observations :

Associativity of addition: We have

$$[(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f)$$
$$= ([a + c] + e, [b + d] + f) = (a + [c + e], b + [d + f])$$
$$= (a, b) + (c + e, d + f) = (a, b) + [(c, d) + (e, f)].$$

Commutativity of addition : We have

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b).$$

Existence of additive identity : We have $(0, 0) \in \mathbf{C}$.

Also $$(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b).$$

$\therefore$ (0, 0) is the additive identity.

Existence of additive inverse : If $(a, b) \in \mathbf{C}$, then $(-a, -b) \in \mathbf{C}$. We have

$$(-a, -b) + (a, b) = (-a + a, -b + b) = (0, 0).$$

$\therefore$ $(-a, -b)$ is the additive inverse of (a, b).

Associativity of multiplication : We have

$$[(a, b)(c, d)](e, f) = (ac - bd, bc + ad)(e, f)$$
$$= ([ac - bd]e - [bc + ad]f, [bc + ad]e + [ac - bd]f)$$
$$= (a[ce - df] - b[de + cf], b[ce - df] + a[de + cf])$$
$$= (a, b)(ce - df, de + cf) = (a, b)[(c, d)(e, f)].$$

Distributive laws : We have $(a, b)[(c, d) + (e, f)] = (a, b)(c + e, d + f)$

$$= (a[c + e] - b[d + f], b[c + e] + a[d + f])$$

$$= ([ac - bd] + [ae - bf], [bc + ad] + [be + af])$$

$$= (ac - bd, bc + ad) + (ae - bf, be + af) = (a, b)(c, d) + (a, b)(e, f).$$

Similarly we can show that the other distributive law also holds good.

Therefore **C** is a ring with respect to the two compositions. The ordered pair (0, 0) is the zero element of the ring.

Commutativity of multiplication : We have

$$(a, b)(c, d) = (ac - bd, bc + ad) = (ca - db, da + cb) = (c, d)(a, b).$$

Existence of multiplicative identity : We have $(1, 0) \in \mathbf{C}$. If $(a, b) \in \mathbf{C}$, then

$$(a, b)(1, 0) = (a1 - b0, b1 + a0) = (a, b) = (1, 0)(a, b).$$

Therefore (1, 0) is the unity element of the ring.

Existence of multiplicative inverse of each non-zero element of C : Let (a, b) be any non-zero element of **C**. Then a and b are not both simultaneously zero. If (c, d) is the multiplicative inverse of (a, b), then we should have

$$(a, b)(c, d) = (1, 0) \quad \text{or} \quad (ac - bd, bc + ad) = (1, 0).$$

By the definition of the equality of two ordered pairs, we have $ac - bd = 1$ and $bc + ad = 0$.

Solving these equations for c, d, we get $c = \dfrac{a}{a^2 + b^2}, d = \left(\dfrac{-b}{a^2 + b^2}\right)$.

Now $a \neq 0$ or $b \neq 0 \Rightarrow a^2 + b^2 \neq 0$. Therefore either c or d or both are non-zero real numbers. Thus $\left(\dfrac{a}{a^2 + b^2}, -\dfrac{b}{a^2 + b^2}\right)$ is the multiplicative inverse of (a, b). Hence **C** is a field.

Note : In this question **C** is nothing but the set of complex numbers defined as ordered pairs of real numbers. Thus we have proved that the set of complex numbers is a field with respect to addition and multiplication of complex numbers.

Problem 5: *Is every field also a division ring? Does the set of all integers under usual addition and multiplication form a field? Give some example of a field which is finite.*

Solution: First give the definitions of a field and a division ring.

For these definitions refer articles 7 and 8.

From these two definitions we conclude that every field is also a division ring.

The set of integers **I** under usual addition and multiplication is a ring. The ring of integers $(\mathbf{I}, +, \bullet)$ is a commutative ring with unity element the integer 1. But this ring is not a field. In this ring the only inversible elements are 1 and – 1 while in a field every non-zero element must be inversible.

Example of a finite field: The ring $(\{0, 1, 2\}, +_3, \times_3)$ is an example of a finite field because the number of distinct elements in this ring is 3 and so it is a finite ring. This ring is a commutative ring with unity element the integer 1. The zero element of this ring is the integer 0. Both the non-zero elements 1 and 2 of this ring possess multiplicative inverse. The multiplicative inverse of 1 is 1 because $1 \times_3 1 = 1$ and the multiplicative inverse of 2 is 2 because $2 \times_3 2 = 1$.

Hence $(\{0, 1, 2\}, +_3, \times_3)$ is a field and it is a finite field.

Problem 6: *Prove that the set of integers R, $R = \{0, 1, 2, 3, 4\}$ forms a field under addition modulo 5 and multiplication modulo 5.* **(Kumaun 2008)**

Solution: Proceed as in problem 7(i). Prepare the composition tables for R for $+_5$ and $\times_5$.

Here also 0 is identity for the operation $+_5$. Also for the operation $+_5$, the inverses of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively.

1 is multiplicative identity *i.e.*, identity for the operation $\times_5$. Also for the operation $\times_5$ the inverses of the non-zero elements 1, 2, 3, 4 of R are 1, 3, 2, 4 respectively.

Problem 7: *(i) Prove that the set* $\{0, 1, 2\}$ *(mod* 3*) is a field with respect to addition and multiplication.*

(ii) Prove that the ring $\mathbf{I}_3$ *of integers modulo* 3 *is a field.*

(iii) Prove that the set $\{0, 1\}$ *(mod* 2*) is a field with respect to addition and multiplication.*

Solution: (i) Let $R = \{0, 1, 2\}$. To prove that $(R, +_3, \times_3)$ is a field.

First we shall show that $(R, +_3)$ is an abelian group. The composition table for R for the operation $+_3$ is as given below.

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Now proceed as in Example 2.

From the composition table we see that R is closed for $+_3$ and the operation $+_3$ on the set R is commutative. The operation $+_3$ on the set R is also associative as we know it.

The element $0 \in R$ is identity for $+_3$. The inverses of 0, 1, 2 for $+_3$ are 0, 2, 1 respectively.

Therefore $(R, +_3)$ is an abelian group.

Now we prepare composition table for R for the operation $\times_3$.

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

From the composition table we see that R is closed for $\times_3$ and the operation $\times_3$ on the set R is commutative.

The operation $\times_3$ on the set R is associative. For if $a, b, c \in R$, then

$$a \times_3 (b \times_3 c) = (a \times_3 b) \times_3 c \text{ because } a(bc) = (ab)c.$$

Also the operation $\times_3$ distributes over the operation $+_3$. For if $a, b, c \in R$, then

$$a \times_3 (b +_3 c) = (a \times_3 b) +_3 (a \times_3 c)$$

and $$(b +_3 c) \times_3 a = (b \times_3 a) +_3 (c \times_3 a).$$

The element $1 \in R$ is identity for the operation $\times_3$ because from the composition table we see that

$$1 \times_3 a = a = a \times_3 1, \ \forall \ a \in R.$$

Also each non-zero element of R possesses multiplicative inverse. From the composition table we see that the inverses of the non-zero elements 1 and 2 of R for $\times_3$ are 1 and 2 respectively.

Thus $(R, +_3, \times_3)$ is a commutative ring with unity element 1 and each non-zero element of R is inversible. Hence $(R, +_3, \times_3)$ is a field.

(ii) We have to prove that $(\mathbf{I}_3, +_3, \times_3)$ is a field where $\mathbf{I}_3 = \{0, 1, 2\}$.

Proceed as in part (i).

(iii) Do yourself. Proceed as in part (i).

Problem 8: *(i) If a, b are any elements of a ring R, prove that* $-(-a) = a$.

(Meerut 2000)

(ii) If two operations $*$ *and* o *on the set I of integers are defined as follows:*

$$a * b = a + b - 1, \ a \ o \ b = a + b - ab,$$

prove that the system $(\mathbf{I}, *, o)$ *is a commutative ring with identity.*

(iii) If R is a ring with unity element 1, *then* $(-1)\, a = -a = a\,(-1) \ \forall \ a \in R$ *and* $(-1)(-1) = 1$.

(Meerut 2000)

Solution: (i) Since R is a group with respect to addition, therefore $-(-a) = a$.

[Remember that in a group $(a^{-1})^{-1} = a$].

(ii) First we shall show that the algebraic structure $(\mathbf{I}, *)$ is an abelian group.

I is closed for the operation $*$: Let $a, b \in \mathbf{I}$.

Then $a * b = a + b - 1$ which is also a member of **I.** Therefore **I** is closed with respect to the operation *.

Commutativity and associativity of the operation $*$ on the set I: Let $a, b, c \in \mathbf{I}$. Then

$$a * b = a + b - 1 = b + a - 1 = b * a$$

and $$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + (b + c - 1) - 1$$
$$= a * (b + c - 1) = a * (b * c).$$

Thus the operation * on the set **I** is commutative as well as associative.

Existence of identity for the operation $*$ on I:

The integer $e \in \mathbf{I}$ will be the identity for the operation $*$ on the set **I** if

$$e * a = a \ \forall \ a \in \mathbf{I}. \qquad \text{[Note that } e * a = a * e\text{]}$$

Now $$e * a = a \ \Rightarrow \ e + a - 1 = a \ \Rightarrow \ e - 1 = 0 \ \Rightarrow \ e = 1.$$

Therefore the integer 1 is identity for the operation * on the set **I** and will be the zero element of the ring $(\mathbf{I}, *, o)$.

Existence of inverse of each element of I for the operation $*$:

Let $a \in \mathbf{I}$. Then $b \in \mathbf{I}$ will be the inverse of a for the operation * if $a * b = 1$.

Now $a * b = 1 \Rightarrow a + b - 1 = 1 \Rightarrow b = 2 - a.$

Thus if $a \in \mathbf{I}$, then $2 - a \in \mathbf{I}$ and is the inverse of a for the operation $*$.

$\therefore$ $(\mathbf{I}, *)$ is an abelian group.

I is closed for the operation o: Let $a, b \in \mathbf{I}$.

Then $a \, o \, b = a + b - ab$ which is also an integer. Therefore **I** is closed with respect to the operation o.

Commutativity and associativity of the operation o on the set I: Let $a, b, c \in \mathbf{I}$. Then

$$a \, o \, b = a + b - ab = b + a - ba = b \, o \, a.$$

Also $(a \, o \, b) \, o \, c = (a + b - ab) \, o \, c = (a + b - ab) + c - (a + b - ab) \, c$

$$= a + b + c - ab - ac - bc + abc$$

and $a \, o \, (b \, o \, c) = a \, o \, (b + c - bc) = a + (b + c - bc) - a \, (b + c - bc)$

$$= a + b + c - bc - ab - ac + abc.$$

$\therefore$ $a \, o \, (b \, o \, c) = (a \, o \, b) \, o \, c.$

Thus the operation o on the set **I** is commutative as well as associative.

Distributivity of o over $*$: Let $a, b, c \in \mathbf{I}$. Then

$$a \, o \, (b * c) = a \, o \, (b + c - 1) = a + (b + c - 1) - a \, (b + c - 1)$$

$$= a + b + c - 1 - ab - ac + a = 2a + b + c - ab - ac - 1.$$

Also $(a \, o \, b) * (a \, o \, c) = (a + b - ab) * (a + c - ac)$

$$= a + b - ab + a + c - ac - 1 = 2a + b + c - ab - ac - 1.$$

$\therefore$ $a \, o \, (b * c) = (a \, o \, b) * (a \, o \, c).$

Similarly we can show that the other distributive law

$$(b * c) \, o \, a = (b \, o \, a) * (c \, o \, a)$$

also holds good.

Existence of identity for the operation o on I:

The integer $u \in \mathbf{I}$ will be the identity for the operation o on the set **I** if

$$u \, o \, a = a \ \forall \ a \in \mathbf{I}.$$ [Note that $u \, o \, a = a \, o \, u$]

Now $u \, o \, a = a \ \forall \ a \in \mathbf{I}$

$\Rightarrow$ $u + a - ua = a \ \forall a \in \mathbf{I}$

$\Rightarrow$ $u(1 - a) = 0 \ \forall a \in \mathbf{I}$

$\Rightarrow$ $u = 0.$

Therefore the integer 0 is the identity for the operation o on the set **I** and so will be the unity element of this ring with unity. We observe that $\forall \ a \in \mathbf{I}$, we have

$$0 \, o \, a = 0 + a - 0 \ a = a = a \, o \, 0.$$

Hence the algebraic structure $(\mathbf{I}, *, o)$ is a commutative ring with identity. The operation $*$ is the addition of this ring and the operation o is the multiplication of this ring. The integer 1 is the zero element of this ring and the integer 0 is the unity element of this ring with unity.

(iii) Let R be a ring with unity element 1. Let a be any element of R.

We have $0\ a = 0$

$\Rightarrow$ $(-1+1)\ a = 0$ $[\because\ -1+1=0]$

$\Rightarrow$ $(-1)\ a + 1a = 0$ [By a dist. law]

$\Rightarrow$ $(-1)\ a + a = 0$ $[\because\ 1a = a]$

$\Rightarrow$ $(-1)\ a = -a.$

Again $a0 = 0 \Rightarrow a(-1+1) = 0 \Rightarrow a(-1) + a1 = 0$

$\Rightarrow$ $a(-1) + a = 0 \Rightarrow a(-1) = -a.$

Hence $(-1)\ a = -a = a(-1)\ \forall\ a \in R.$

Now $(-1)(-1) = -(-1)$ $[\because (-1)\ a = -a,$ as proved above$]$

$= 1.$ $[\because$ in a ring, $-(-a) = a]$

Problem 9: *Prove that the set of rational numbers with two operations * and o defined by*

$a * b = a + b - 1,\ a\ o\ b = a + b - ab$ *is a field.* **[Meerut 2000]**

Solution: Proceed as in problem 8(ii).

Problem 10: *If addition and multiplication modulo* 10 *is defined on the set of integers* $R = \{0, 2, 4, 6, 8\}$, *prove that the resulting system is a ring with unity. Is it an integral domain?*

Solution: We have $R = \{0, 2, 4, 6, 8\}$. To prove that $(R, +_{10}, \times_{10})$ is a ring with unity.

First we shall show that $(R, +_{10})$ is an abelian group. The composition table for R for the operation $+_{10}$ is as given below.

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

We see that all the entries in the composition table are elements of the set R. Therefore R is **closed** with respect to $+_{10}$.

The composition $+_{10}$ on the set R is **commutative.** For if $a, b \in R$, then

$a +_{10} b$ = least non-negative remainder when $a + b$ is divided by 10

= least non-negative remainder when $b + a$ is divided by 10

$= b +_{10} a.$

The composition $+_{10}$ on the set R is **associative.** For if $a, b, c \in R$, then

$a +_{10} (b +_{10} c) = (a +_{10} b) +_{10} c$ because $a + (b + c) = (a + b) + c.$

Existence of additive identity: We have $0 \in R$

and $0 +_{10} a = a = a +_{10} 0,\ \forall\ a \in R.$

$\therefore$ 0 is the identity for the operation $+_{10}$ and will be the zero element of the ring $(R, +_{10}, \times_{10})$.

Existence of additive inverse: From the composition table we see that the inverses of 0, 2, 4, 6, 8 for the operation $+_{10}$ are 0, 8, 6, 4, 2 respectively. Thus each element of R possesses inverse for $+_{10}$.

$\therefore$ $(R, +_{10})$ is an abelian group.

Now we prepare the composition table for R for the operation $\times_{10}$.

$\times_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

We see that all the entries in the composition table are elements of the set R. Therefore R is closed with respect to $\times_{10}$.

The operation $\times_{10}$ on the set R is associative. For if $a, b, c \in R$, then

$$a \times_{10} (b \times_{10} c) = (a \times_{10} b) \times_{10} c \text{ because } a(bc) = (ab)c.$$

Also the operation $\times_{10}$ distributes over the operation $+_{10}$. For if $a, b, c \in R$, then

$$a \times_{10} (b +_{10} c) = (a \times_{10} b) +_{10} (a \times_{10} c)$$

and $$(b +_{10} c) \times_{10} a = (b \times_{10} a) +_{10} (c \times_{10} a).$$

$\therefore$ the algebraic structure $(R, +_{10}, \times_{10})$ is a ring. The zero element of this ring is 0 which is identity for the operation $+_{10}$.

This ring is a ring with unity because it possesses multiplicative identity. From the composition table for $\times_{10}$ we see that $6 \in R$ is identity for the operation of multiplication modulo 10. We have

$$6 \times_{10} a = a = a \times_{10} 6, \ \forall a \in R.$$

Thus 6 is identity for the operation $\times_{10}$ and is therefore the unity element of the ring $(R, +_{10}, \times_{10})$.

The operation $\times_{10}$ on the set R is commutative because the corresponding rows and columns in the composition table of R for the operation $\times_{10}$ are identical. Thus

$$a \times_{10} b = b \times_{10} a, \ \forall a, b \in R.$$

Also from the composition table of R for the operation $\times_{10}$ we observe that the product of no two non-zero elements of R is the zero element of R. Thus if $a, b \in R$, then

$$a \times_{10} b = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

$\therefore$ the ring $(R, +_{10}, \times_{10})$ does not possess zero divisors.

Since $(R, +_{10}, \times_{10})$ is a commutative ring with unity and without zero divisors, therefore it is an integral domain.

Problem 11: *Do the following sets form integral domains with respect to ordinary addition and multiplication? If so, state if they are fields.*

(*i*) *The set of numbers of the form* $b\sqrt{2}$ *with* b *rational.*

(*ii*) *The set of even integers.*

(*iii*) *The set of positive integers.*

Solution: (i) Let $A = \{b\sqrt{2} : b \in \mathbf{Q}\}$.

We have $3\sqrt{2} \in A$ and $5\sqrt{2} \in A$. Then $(3\sqrt{2})(5\sqrt{2}) = 30$.

Now 30 cannot be put in the form $b\sqrt{2}$ where b is a rational number. Therefore $30 \notin A$. Thus A is not closed with respect to multiplication. Therefore the question of A becoming a ring does not arise.

(ii) Let R be the set of all even integers. Then R is a ring with respect to addition and multiplication of integers. Also the multiplication is a commutative composition. R is without zero divisors since the product of two non-zero even integers cannot be equal to zero which is the zero element of this ring. Since the integer $1 \notin R$, therefore R is a ring without unity.

R will be an integral domain if we do not require the existence of the unit element for an integral domain.

But R is not a field since the multiplicative identity does not exist.

(iii) Let N be the set of positive integers. Since the integer $0 \notin N$, therefore the additive identity does not exist. So N will not be a ring.

Problem 12: *If a ring R has a left identity as well as right identity, then prove that the two are equal.*

Solution: Let R be a ring which possesses left identity e and right identity e'

i.e., $ea = a \ \forall\, a \in R$ and $ae' = a \ \forall\, a \in R$.

To prove that $e = e'$.

Since e is left identity and $e' \in R$, therefore

$$e\,e' = e'. \qquad \ldots(1)$$

Again e' is right identity and $e \in R$.

$$\therefore \quad e\,e' = e. \qquad \ldots(2)$$

Since $e\,e'$ is a unique element of R, therefore from (1) and (2) we conclude that $e = e'$.

Problem 13: *Prove that the only idempotent elements of an integral domain with unity are* 0 *and* 1.

Solution: Let R be an integral domain with unity 1.

Let $a \in R$ and a be idempotent *i.e.*, $a^2 = a$.

We have $a^2 = a \Rightarrow aa = a1 \Rightarrow aa - a1 = 0 \Rightarrow a(a-1) = 0$.

But in an integral domain the product of two elements is 0 only if at least one of them is zero.

$$\therefore \quad a(a-1) = 0 \Rightarrow a = 0 \quad \text{or} \quad a - 1 = 0$$

$\Rightarrow \qquad a = 0 \quad$ or $\quad a = 1.$

Hence the only idempotent elements of an integral domain with unity are 0 and 1.

Problem 14: *An element a of a ring R is said to be* ***nilpotent*** *if* $a^n = 0$ *for some positive integer n. Prove that* $a = 0$ *is the only nilpotent element of an integral domain.*

Solution: Let R be an integral domain. We have $0^n = 0$ for every positive integer n.

$\therefore$ The element 0 of R is surely nilpotent.

Now let a be any non-zero element of R. Since in an integral domain the product of two non-zero elements cannot be zero, therefore

$$a \neq 0 \Rightarrow a^2 = aa \neq 0 \Rightarrow a^3 = aa^2 \neq 0 \Rightarrow a^4 = aa^3 \neq 0, \text{ and so on.}$$

Thus in an integral domain if $a \neq 0$, then $a^n \neq 0$ for every positive integer n and so a cannot be nilpotent.

Hence 0 is the only nilpotent element of an integral domain.

Problem 15: *(i) If R is a commutative ring , prove by induction that*

$$(a + b)^n = a^n + {}^nC_1\, a^{n-1} b + {}^nC_2\, a^{n-2} b^2 + \ldots + b^n$$

for every positive integer n; here a and b are elements of R.

(ii) Prove that a ring R is commutative if and only if

$$(a + b)^2 = a^2 + 2ab + b^2 \quad \forall\, a, b \in R.$$ **(Gorakhpur 2012; Kumaun 12)**

Solution: (i) We have $a + b = a^1 + b^1$.

Now
$$\begin{aligned}(a + b)^2 &= (a + b)(a + b) \\ &= a^2 + ab + ba + b^2, \text{ by dist. laws} \\ &= a^2 + ab + ab + b^2 \\ &\qquad [\because\ ab = ba, \text{ the ring } R \text{ being commutative}] \\ &= a^2 + 2\,ab + b^2 \\ &= a^2 + {}^2C_1\, ab + b^2.\end{aligned}$$

Thus the result is true for $n = 2$.

Now assume that the result is true for any positive integer n *i.e.*,

$$(a + b)^n = a^n + {}^nC_1\, a^{n-1} b + \ldots + {}^nC_r\, a^{n-r} b^r + {}^nC_{r+1}\, a^{n-r-1} b^{r+1} + \ldots + b^n.$$

Then
$$\begin{aligned}(a + b)^{n+1} &= (a + b)(a + b)^n \\ &= (a + b)(a^n + {}^nC_1\, a^{n-1} b + {}^nC_2\, a^{n-2} b^2 + \ldots \\ &\qquad + {}^nC_r\, a^{n-r} b^r + {}^nC_{r+1}\, a^{n-r-1} b^{r+1} + \ldots + b^n) \\ &= a^{n+1} + (ba^n + {}^nC_1 a^n b) + \ldots \\ &\qquad + ({}^nC_r\, ba^{n-r} b^r + {}^nC_{r+1}\, a^{n-r} b^{r+1}) + \ldots + b^{n+1}.\end{aligned}$$

Since the ring R is commutative, therefore

$$ba^n = a^n b, ba^{n-r} b^r = (ba^{n-r}) b^r = (a^{n-r} b) b^r$$
$$= a^{n-r} b b^r = a^{n-r} b^{r+1}.$$

Also $1 = {}^nC_0$, ${}^nC_r + {}^nC_{r+1} = {}^{n+1}C_{r+1}$.

Hence
$$(a+b)^{n+1} = a^{n+1} + ({}^nC_0 + {}^nC_1) a^n b + \ldots$$
$$+ ({}^nC_r + {}^nC_{r+1}) a^{n-r} b^{r+1} + \ldots + b^{n+1}$$
$$= a^{n+1} + {}^{n+1}C_1 a^{(n+1)-1} b + \ldots$$
$$+ {}^{n+1}C_{r+1} a^{(n+1)-(r+1)} b^{r+1} + \ldots + b^{n+1}.$$

Thus the result is true for $n+1$, if it is true for n. But it is true for $n = 1$ and $n = 2$. Hence by induction it is true for all positive integral values of n.

(ii) Let R be a commutative ring *i.e.*, $ab = ba \ \forall\, a, b \in R$.

Then to prove that $(a+b)^2 = a^2 + 2ab + b^2 \ \forall\, a, b \in R$.

Let $a, b \in R$.

We have
$$(a+b)^2 = (a+b)(a+b) \qquad [\because\ a^2 = aa]$$
$$= aa + ab + ba + bb, \text{ by dist. laws}$$
$$= a^2 + ab + ab + b^2 \qquad [\because\ ba = ab]$$
$$= a^2 + 2ab + b^2.$$

Hence if R is commutative ring, then $(a+b)^2 = a^2 + 2ab + b^2 \ \forall\ a, b \in R$.

Conversely suppose that $(a+b)^2 = a^2 + 2ab + b^2 \ \forall\, a, b \in R$. Then to prove that R is a commutative ring.

Let $a, b \in R$. Then
$$(a+b)^2 = a^2 + 2ab + b^2$$
$$\Rightarrow \quad (a+b)(a+b) = a^2 + 2ab + b^2$$
$$\Rightarrow \quad a^2 + ab + ba + b^2 = a^2 + 2ab + b^2, \text{ by dist. laws}$$
$$\Rightarrow \quad ab + ba = 2ab, \text{ by left and right cancellation laws for addition in } R$$
$$\Rightarrow \quad ab + ba = ab + ab \qquad [\because\ ab + ab = 2ab]$$
$$\Rightarrow \quad ba = ab, \text{ by left cancellation law for addition in } R.$$

Thus $ab = ba \ \forall\, a, b \in R$ and so R is a commutative ring.

Problem 16: *Explain with examples the difference between a field, a skew field and an integral domain.*

Solution: First give the definitions of a field, a skew field and an integral domain. For these definitions refer articles 7 and 8.

Difference between a field and a skew-field: Every field is a skew-field but a skew-field need not be a field. A skew field will be a field only if the operation of multiplication in it is commutative. The skew field given in problem 17 part (iv) is not a field because the operation of multiplication of matrices in this skew field is not commutative.

Difference between a field and an integral domain: Every field is an integral domain but every integral domain need not be a field. For example the field of rational numbers $(\mathbf{Q}, +, \bullet)$ is an integral domain because it does not possess zero divisors. The

product of two non-zero rational numbers is never zero. On the other hand, the ring of integers $(\mathbf{I}, +, \bullet)$ is an integral domain but it is not a field. The only inversible elements of this ring are 1 and – 1 while in a field every non-zero element must be inversible.

However, every finite integral domain is always a field. For example, the ring $(\{0, 1, 2\}, +_3, \times_3)$ is an integral domain and it is also a field.

Difference between an integral domain and a skew field: A skew field need not be an integral domain because in a skew field multiplication need not be commutative while in an integral domain multiplication must be commutative. Also an integral domain need not be a skew field. For example, the ring of integers is an integral domain but it is not a skew field.

Problem 17: *Give an example each of :*

(*i*) *a commutative ring without unity,*

(*ii*) *a non-commutative ring ,*

(*iii*) *a ring without zero divisors,*

(*iv*) *division ring.*

Solution: (i) **A commutative ring without unity:** See problem 3(ii).

(ii) **A non-commutative ring:** See problem 3(i).

(iii) **A ring without zero divisors:** The ring of integers $(\mathbf{I}, +, \bullet)$ is a ring without zero divisors. We know that the product of two non-zero integers is never zero. Thus if $a, b \in \mathbf{I}$, then

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0.$$

Hence the ring of integers is a ring without zero divisors.

(iv) **Division ring:** Let M be the set of all 2×2 matrices of the form

$$\begin{bmatrix} a + ib & c + id \\ -c + id & a - ib \end{bmatrix},$$

where a, b, c, d are arbitrary real numbers.

Then M is a ring for addition and multiplication of matrices as the two ring operations. This ring possesses unity element. The unit matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M$ and we have

$$IA = A = AI, \ \forall A \in M.$$

Also in this ring every non-zero element possesses multiplicative inverse. But the operation of multiplication of matrices on the set M is not commutative. Hence the above ring M is a division ring or a skew field.

Problem 18: *If in a ring with unity any element a has the multiplicative inverse, then a cannot be a divisor of zero.*

Solution: Let R be a ring with unity 1.

Let $a \in R$ be such that a has multiplicative inverse. To prove that a cannot be a divisor of zero.

Let $b \in R$ be such that $ab = 0$ or $ba = 0$. Then a cannot be a divisor of zero if we prove that $ab = 0$ or $ba = 0$ is possible only if $b = 0$.

We have $ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0$

$[\because a^{-1}$ exists $]$

$\Rightarrow (a^{-1}a)b = 0 \Rightarrow 1b = 0 \Rightarrow b = 0.$

Again $ba = 0 \Rightarrow (ba)a^{-1} = 0a^{-1} \Rightarrow b(aa^{-1}) = 0 \Rightarrow b1 = 0 \Rightarrow b = 0.$

Hence a cannot be a zero divisor.

Problem 19: *If a, b, c, d are any elements of a ring R, prove that*

(i) $a - b = c - d \Leftrightarrow a + d = b + c.$

(ii) $(a - b)(c - d) = (ac + bd) - (ad + bc).$ **(Kumaun 2007)**

Solution: (i) We have $a - b = c - d$

$\Leftrightarrow a + (-b) = c + (-d)$

$\Leftrightarrow a + (-b) + d = c + (-d) + d$

$\Leftrightarrow a + d + (-b) = c + 0$ $[\because$ in a ring addition is commutative as well as associative and $-d + d = 0]$

$\Leftrightarrow a + d + (-b) = c$ $[\because c + 0 = c]$

$\Leftrightarrow a + d + (-b) + b = c + b$

$\Leftrightarrow a + d + 0 = c + b \Leftrightarrow a + d = c + b.$

(ii) We have $(a - b)(c - d) = (a - b)c - (a - b)d$ $[\because a(b - c) = ab - ac]$

$= (ac - bc) - (ad - bd) = (ac - bc) - ad + bd$

$= (ac + bd) - bc - ad$ $[\because$ Addition is commutative and associative$]$

$= (ac + bd) - (bc + ad).$

Problem 20: *Prove that in a field*

(i) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ (ii) $\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}$

(iii) $(-a)^{-1} = -(a^{-1})$ (iv) $\frac{(-a)}{(-b)} = \frac{a}{b}.$

Solution: Let $a, b, c, d \in F$ where F is a field. Here $b \neq 0, d \neq 0.$

(i) We have $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ab^{-1} = cd^{-1} \Leftrightarrow (ab^{-1})(bd) = (cd^{-1})(bd)$

$\Leftrightarrow (ad)(b^{-1}b) = (bc)(d^{-1}d)$ $[\because$ in a field multiplication is commutative as well as associative$]$

$\Leftrightarrow (ad)1 = (bc)1 \Leftrightarrow ad = bc.$

(ii) We have $\frac{a}{b} - \frac{c}{d} = (ab^{-1}) - (cd^{-1}) = (bd)^{-1}(bd)[(ab^{-1}) - (cd^{-1})]$

$= (bd)^{-1}[(bd)(ab^{-1}) - (bd)(cd^{-1})]$

$= (bd)^{-1}(ad - bc) = \frac{ad - bc}{bd}.$

(iii) We have $(-a)[-(a^{-1})] = aa^{-1}$ $[\because$ in a field $(-a)(-b) = ab]$

$= 1.$

$\therefore$ $(-a)^{-1} = -(a^{-1}).$ $[\because$ in a field $ab = 1 \Rightarrow a^{-1} = b]$

(iv) We have $\frac{(-a)}{(-b)} = (-a)(-b)^{-1} = (-a)[-(b^{-1})]$

[$\because$ By part (iii) of this question $(-b)^{-1} = -(b^{-1})$]

$= ab^{-1}$ [$\because$ in a field $(-a)(-b) = ab$]

$= \frac{a}{b}$.

Problem 21: *(i) Show that $Z[\sqrt{-5}]$, the set of complex numbers $a + b\sqrt{(-5)}$ where a, b are integers, is an integral domain.*

(ii) Prove that the set $I(\sqrt{2})$ of numbers of the form $a + b\sqrt{2}$, with a and b as integers is an integral domain with respect to ordinary addition and multiplication. Is it a field ?

(Kumaun 2008)

Solution: (i) Let $a + b\sqrt{(-5)}$ and $c + d\sqrt{(-5)}$ be any two complex numbers belonging to the set $Z[\sqrt{(-5)}]$, where a, b, c, d are any integers.

Then $[a + b\sqrt{(-5)}] + [c + d\sqrt{(-5)}] = (a + c) + (b + d)\sqrt{(-5)}$

and $[a + b\sqrt{(-5)}][c + d\sqrt{(-5)}] = (ac - 5bd) + (ad + bc)\sqrt{(-5)}$.

These are again members of the set $Z[\sqrt{-5}]$ because $a + c, b + d, ac - 5bd, ad + bc$ are all integers. Therefore $Z[\sqrt{-5}]$ is closed with respect to ordinary addition and multiplication of complex numbers.

Further in complex numbers both addition and multiplication are associative as well as commutative compositions. Also multiplication distributes with respect to addition. The complex number $0 + 0\sqrt{(-5)}$ is a member of the set $Z[\sqrt{-5}]$ and is the additive identity. The additive inverse of $a + b\sqrt{(-5)} \in Z[\sqrt{-5}]$ is $(-a) + (-b)\sqrt{(-5)}$. The complex number $1 + 0\sqrt{(-5)}$ is a member of the set $Z[-\sqrt{5}]$ and is the multiplicative identity.

Therefore the set of complex numbers $a + b\sqrt{(-5)}$ where a, b are integers is a commutative ring with unity for the addition and multiplication of complex numbers as the two ring compositions.

Also this ring is free from zero divisors since the product of two non-zero complex numbers cannot be zero. Therefore $Z[\sqrt{-5}]$ is an integral domain for ordinary addition and multiplication of complex numbers as the two ring compositions.

(ii) As in Example 7, we can easily verify that the given system is a commutative ring with unit element $1 + 0\sqrt{2}$. Also $0 + 0\sqrt{2}$ is the zero element of this ring. Now in order to prove that this ring is an integral domain, we should prove that this ring is without zero divisors.

Let $a + b\sqrt{2}$ and $c + d\,2$ be any two elements of this ring. Then

$(a + b\sqrt{2})(c + d\sqrt{2}) = 0 + 0\sqrt{2}$

$\Rightarrow$ $ac + 2bd = 0$ and $bc + ad = 0$

and this will happen only when either

$a = 0$ and $b = 0$ or $c = 0$ and $d = 0$.

Thus $(a + b\sqrt{2})(c + d\sqrt{2}) = 0 + 0\sqrt{2}$

$\Rightarrow$ either $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$.

Thus the given ring is without zero divisors. Therefore it is an integral domain. But it is not a field. Obviously $5 + 3\sqrt{2}$ is a non-zero element of this ring. Its inverse would have been

$$\frac{1}{5+3\sqrt{2}} = \frac{5-3\sqrt{2}}{(5+3\sqrt{2})(5-3\sqrt{2})} = \frac{5-3\sqrt{2}}{7} = \frac{5}{7} - \frac{3}{7}\sqrt{2}$$

which is not an element of this ring.

Problem 22: *(i) Prove that the totality R of all ordered pairs (a, b) of real numbers is a commutative ring with zero divisors under the addition and multiplication of ordered pairs defined as*

$$(a, b) + (c, d) = (a + c, b + d),\ (a, b)(c, d) = (ac, bd)\ \forall\ (a, b), (c, d) \in R.$$

(ii) Define a ring and an integral domain. Give an example of a ring which is not an integral domain.

Solution: (i) We see that R is closed with respect to the two compositions since $a + c$, $b + d, ac, bd$ are all real numbers. Now let $(a, b), (c, d), (e, f)$ be any elements of R. Then we observe :

Associativity of addition: We have

$$[(a, b) + (c, d)] + (e, f) = (a + c, b + d) + (e, f)$$
$$= ([a + c] + e, [b + d] + f)$$
$$= (a + [c + e], b + [d + f])$$
[$\because$ Addition of real numbers is associative]
$$= (a, b) + (c + e, d + f)$$
$$= (a, b) + [(c, d) + (e, f)].$$

$\therefore$ addition in R is associative.

Commutativity of addition: We have

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b).$$

Existence of additive identity: We have $(0, 0) \in R$.

Also $(0, 0) + (a, b) = (0 + a, 0 + b) = (a, b)$.

Existence of additive inverse: If $(a, b) \in R$, then $(-a, -b) \in R$ and we have

$$(-a, -b) + (a, b) = (-a + a, -b + b) = (0, 0).$$

$\therefore$ $(-a, -b)$ is the additive inverse of (a, b).

Associativity of Multiplication: We have

$$[(a, b)(c, d)](e, f) = (ac, bd)(e, f) = ([ac]e, [bd]f)$$
$$= (a[ce], b[df])$$
[$\because$ Multiplication of real numbers is associative]
$$= (a, b)(ce, df) = (a, b)[(c, d)(e, f)].$$

Distributive laws: We have

$$(a, b)[(c, d) + (e, f)] = (a, b)(c + e, d + f)`$$
$$= (a[c + e], b[d + f])$$
$$= (ac + ae, bd + bf) = (ac, bd) + (ae, bf)$$
$$= (a, b)(c, d) + (a, b)(e, f).$$

Similarly we can show that the other distributive law also holds good.

$\therefore$ R is a ring with respect to the given compositions.

Commutativity of multiplication: We have

$$(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b).$$

$\therefore$ R is a commutative ring.

Existence of multiplicative identity: We have $(1, 1) \in R$. If $(a, b) \in R$, then

$$(1, 1)(a, b) = (1a, 1b) = (a, b) = (a, b)(1, 1).$$

$\therefore$ $(1, 1)$ is the multiplicative identity and is therefore the unit element of the ring. So R is a ring with unity also.

The zero element of this ring is the ordered pair $(0, 0)$.

Now in order to show that R is a ring with zero divisors we should show that there exist two non-zero elements of R whose product is equal to the zero element of R. Obviously neither $(3, 0)$ nor $(0, 5)$ is equal to the zero element of R. But $(3, 0)(0, 5) = (3 \times 0, 0 \times 5) = (0, 0)$ which is the zero element of R.

$\therefore$ R is a ring with zero divisors.

(ii) For the definition of a ring refer article 1. and for the definition of an integral domain refer article 6.

For an example of a ring which is not an integral domain consider the ring $(R, +_6, \times_6)$ where $R = \{0, 1, 2, 3, 4, 5\}$.

The above ring $(R, +_6, \times_6)$ is a commutative ring and possesses unity element which is the integer 1. But this ring is not an integral domain because it possesses zero divisors.

We observe that $2 \in R, 3 \in R, 2 \neq 0, 3 \neq 0$, but $2 \times_6 3 = 0$. Thus both 2 and 3 are zero divisors. Hence the ring

$$(\{0, 1, 2, 3, 4, 5\}, +_6, \times_6)$$

is not an integral domain.

Problem 23: *(i) Show that the set of all matrices of the form* $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$*, a and b being real numbers, is a ring with matrix addition and matrix multiplication as the two ring compositions. Is it a commutative ring?* **(Gorakhpur 2014)**

(ii) Show that the set R of all real valued continuous functions defined in the closed interval $[0, 1]$ *is a commutative ring with unity with respect to the addition and multiplication of functions defined point wise as follows :*

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)\, g(x),$$

where f, g are any two members of R.

Solution: (i) Proceed as in example 1.

(ii) If f is a real valued function in the closed interval $[0, 1]$, then we mean that $f(x)$ is a real number $\forall \; x \in [0, 1]$. We know that the sum and product of two real numbers are also real numbers. Also the sum and product of two continuous functions is also a continuous function. Therefore R is closed with respect to the given compositions.

Now let f, g, h be any three elements of R. Then we make the following observations :

Associativity of addition: For every $x \in [0, 1]$, we have

$$[(f+g)+h](x) = [(f+g)(x)] + h(x)$$
$$= [f(x) + g(x)] + h(x)$$
$$= f(x) + [g(x) + h(x)] \quad [\because f(x), g(x), h(x) \text{ are real numbers and addition of real numbers is associative}]$$
$$= f(x) + (g+h)(x) = [f + (g+h)](x).$$

$\therefore$ $(f+g)+h = f+(g+h)$, by the equality of two mappings.

Commutativity of addition: We have

$$(f+g)(x) = f(x) + g(x) = g(x) + f(x)$$
$$[\because \text{Addition of real numbers is commutative}]$$
$$= (g+f)(x).$$

$\therefore$ $f+g = g+f$.

Existence of additive identity: Let us define a function e by the rule

$$e(x) = 0 \quad \forall \quad x \in [0,1].$$

Then $e \in R$. Also if $f \in R$, we have

$$(e+f)(x) = e(x) + f(x) = 0 + f(x) = f(x).$$

$\therefore$ $e + f = f$.

$\therefore$ the function e is the additive identity.

Existence of additive inverse: Let $f \in R$. Let us define a function $-f$ by the formula

$$(-f)(x) = -[f(x)] \quad \forall \quad x \in [0,1].$$

Then $-f \in R$ and we have

$$[-f + f](x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = e(x).$$

$\therefore$ $-f + f = e$.

$\therefore$ the function $-f$ is the additive inverse of f.

Associativity of multiplication: We have

$$[(fg)h](x) = [(fg)(x)]\,h(x) = [f(x)\,g(x)]\,h(x) = f(x)\,[g(x)\,h(x)]$$
$$= f(x)\,[(gh)(x)] = [f(gh)](x).$$

$\therefore$ $(fg)h = f(gh)$.

Distributive laws: We have

$$[f(g+h)](x) = f(x)\,[(g+h)(x)] = f(x)\,[g(x) + h(x)]$$
$$= f(x)\,g(x) + f(x)\,h(x) = (fg)(x) + (fh)(x)$$
$$= [fg + fh](x).$$

$\therefore$ $f(g+h) = fg + fh$.

Similarly we can prove that $(g+h)f = gf + hf$.

$\therefore$ R is a ring with respect to the given compositions.

Commutativity of multiplication: We have

$$(fg)(x) = f(x)\,g(x) = g(x)\,f(x) = (gf)(x).$$

$\therefore$ $fg = gf$.

$\therefore$ R is a commutative ring.

Existence of multiplicative identity: Let us define a function i by the formula

$$i(x) = 1 \quad \forall \quad x \in [0,1].$$

Then $i \in R$. If $f \in R$, we have

$(i f)(x) = i(x)\ f(x) = 1\ f(x) = f(x)$.

$\therefore \quad i f = f = f i$ [By commutativity of multiplication]

$\therefore$ The function i is the multiplicative identity.

Thus the ring R is with unity element.

Comprehensive Problems 2

Problem 1: *Let x, y be commutative elements of a ring R of characteristic two. Show that*

$$(x + y)^2 = x^2 + y^2 = (x - y)^2.$$

Solution: Since the ring R is of characteristic two, therefore

$$a + a = 0 \ \forall\ a \in R.$$

Now let $x, y \in R$ and $x y = y x$.

Then $(x + y)^2 = (x + y)(x + y) = x^2 + x y + y x + y^2$, by dist. laws

$= x^2 + x y + x y + y^2$ [$\because\ x y = y x$]

$= x^2 + 0 + y^2$ [$\because\ x y \in R$ and R is of characteristic two implies $x y + x y = 0$]

$= x^2 + y^2$.

Again $(x - y)^2 = (x - y)(x - y) = x^2 - x y - y x + y^2$

$= x^2 - x y - x y + y^2 = x^2 - (x y + x y) + y^2$

$= x^2 - 0 + y^2 = x^2 + y^2$.

Problem 2: *Let R be a non-zero ring such that for all $a \in R$, $a^2 = a$. Prove that R is a commutative ring of characteristic 2.*

Solution: This question has been completely solved in example 5 .

We have proved there in part (i) of the question that

$$a + a = 0 \ \forall\ a \in R.$$

Therefore the ring R is of characteristic two.

Again in parts (ii) and (iii) of that question we have proved that the ring R is commutative.

Problem 3: *Show that every finite integral domain is of finite characteristic.*

Solution: Let $(R, +, .)$ be a finite integral domain.

Let a be any non-zero element of R. Then we know that the characteristic of the integral domain $(R, +, .)$ is equal to the order of the element a regarded as a member of the additive group of the integral domain *i.e.*, regarded as a member of the additive group $(R, +)$.

[Refer theorem 2 of article 9].

But from our study of the order of an element in the group theory we know that the order of every element of a finite group is finite. Therefore the order of a as a member of the additive group $(R, +)$ is finite.

Hence every finite integral domain is of finite characteristic.

Problem 4: *Show that in an integral domain all non-zero elements generate additive cyclic groups of the same order which is equal to the characteristic of the integral domain.*

Solution: Let D be an integral domain.

First we shall prove that each non-zero element of D, regarded as a member of the additive group of D, is of the same order. For proof refer theorem 3 of article 8.

Now we know that the order of a cyclic group is equal to the order of its generator. Hence in an integral domain all non-zero elements generate additive cyclic groups of the same order.

In the end we shall prove that the characteristic of the integral domain D is equal to the order of any non-zero element of D regarded as a member of the additive group of D. For proof refer theorem 2 of article 8.

Problem 5: *Give without proof, an example of an integral domain which contains only five elements. Is this an ordered integral domain ? Give reason.*

Solution: The integral domain $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$ contains only five elements.

This integral domain is not an ordered integral domain as shown below.

Suppose the above integral domain is an ordered integral domain and P is the set of positive elements of this integral domain. The zero element of this integral domain is 0.

Now 1 is an element of the above integral domain and $1 \neq 0$. The additive inverse of 1 is 4 because $1 +_5 4 = 0 = 4 +_5 1$.

According to the definition of an ordered integral domain either $1 \in P$ or its additive inverse $4 \in P$.

But P is closed with respect to $+_5$.

$\therefore \qquad 1 \in P \Rightarrow 1 +_5 1 +_5 1 +_5 1 \in P \Rightarrow 4 \in P.$

This contradicts the principle of trichotomy.

Similarly $4 \in P \Rightarrow 4 +_5 4 +_5 4 +_5 4 \in P \Rightarrow 1 \in P$. This again contradicts the principle of trichotomy.

Hence the integral domain $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$ is not an ordered integral domain.

Problem 6: *Define the characteristic of a ring and prove that if R is a finite ring then the characteristic of R is finite and $\neq 0$.*

Solution: For the definition of the characteristic of a ring refer article 9.

Let $(R, +, .)$ be a finite ring having n elements.

From our study of group theory we know that if a is any element of a finite group G of order n, then $a^n = e$, where e is the identity of the group.

Now the identity of the additive group $(R, +)$ of the ring $(R, +, .)$ is 0. Therefore if a is any element of R, then we have $na = 0$.

Thus we have $\qquad na = 0 \quad \forall \quad a \in R.$

Therefore the characteristic of the ring R is $\leq n$ and cannot be infinite or zero.

Hence if R is a finite ring then the characteristic of R is finite and $\neq 0$.

Problem 7: *Define an ordered field and illustrate the concept with the help of an example.*

Solution: **Ordered field. Definition:** A field $(F, +, .)$ is said to be ordered if F contains a subset F_+ such that

(i) F_+ is closed with respect to addition and multiplication as defined on F.

(ii) $\forall\ a \in F$, one and only one of $a = 0, a \in F_+, -a \in F_+$ holds **(Principle of Trichotomy).**

The elements of F_+ are called the **positive** elements of F, all other non-zero elements of F are called **negative** elements of F.

An example of an ordered field: The field of real numbers $(\mathbf{R}, +, .)$ is an ordered field. The set $\mathbf{R}_+$ of all positive real numbers is the set of the positive elements of this field. We know that the sum and product of two positive real numbers is again a positive real number *i.e.*, $\mathbf{R}_+$ is closed with respect to addition and multiplication. If $a \in \mathbf{R}$, then either a is zero or positive or negative *i.e.*, either $a = 0$ or $a \in \mathbf{R}_+$ or $-a \in \mathbf{R}_+$.

The field of rational numbers $(\mathbf{Q}, +, .)$ is also an ordered field. But the field of complex numbers $(\mathbf{C}, +, .)$ is not an ordered field.

Hints to Objective Type Questions

Multiple Choice Questions

1. The algebraic structure $(\{0, 1, 2, 3\}, +_4, \times_4)$, is a ring. It is not an integral domain or a field or a skew-field because it possesses zero divisors. We have $2 \times_4 2 = 0$, where $2 \neq 0$. So, 2 is a zero divisor.
2. See Example 6.
3. We have $2 +_5 3 = 0$ *i.e.*, the additive identity of the given ring. So, the additive inverse of 2 is 3.
4. See Example 6.
5. The order of the unit element 1 is zero when regarded as a member of the additive group of $\mathbf{Q}$ so $\mathbf{Q}$ is of characteristic zero.
6. See article 2 part (iv).
7. See article 11, Illustration 2.
8. See article 7.
9. The ring of integers $(Z, +, \bullet)$ is a skew field.
10. See article 7.
11. See article 8.
12. See Problem 6 of Comprehensive Problems 1.
13. See Illustration 1 of article 5.
14. See Problem 23(i) of Comprehensive Problems 1.
15. See Illustration 2 of article 9.

16. See article 10.
17. See Illustration 3 of article 9.
18. See Example 5(i).
19. See Illustration 2 of article 9.
20. See Illustration 2 of article 9.
21. See Illustration 3 of article 4.
22. See Example 6.

Fill in the Blank(s)

1. If the algebraic structure $(R, +, \bullet)$ is a ring, then obviously for the operation of addition, R is an abelian group. Hence, the algebraic structure $(R, +)$ is an abelian group.
2. In a ring the element 0 which is identity for addition is such that $a + 0 = a = 0 + a, \ \forall \ a \in R$. It is called the zero element of the ring.
3. A ring R is said to be a commutative ring if the operation of multiplication on R is commutative *i.e.*, if $ab = ba, \ \forall \ a, b \in R$.
4. A ring R is said to be a ring with unity if there exists an element 1 in R such that
$$1a = a = a1, \ \forall \ a \in R.$$
So, a ring R is said to be a ring with unity if it possesses multiplicative identity.
5. See article 2, Theorem, part (i).
6. See article 2, Theorem, part (iii).
7. See article 5. Definition of ring without zero divisors.
8. We have $(-\frac{3}{7})(-\frac{7}{3}) = 1$ *i.e.*, the multiplicative identity. So, the multiplicative inverse of $-\frac{3}{7}$ is $-\frac{7}{3}$.
9. In the field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$, the zero element *i.e.*, the additive identity is 0 and the unity element *i.e.*, the multiplicative identity is 1.
(i) We have $3 \times_5 2 = 1$. So, the multiplicative inverse of 3 is 2.
(ii) We have $1 +_5 4 = 0$. So, the additive inverse of 1 is 4.
10. The multiplicative inverse of $3 + 4i$
$$= \frac{1}{3+4i} = \frac{3-4i}{(3+4i)(3-4i)} = \frac{3-4i}{9+16} = \frac{3}{25} - \frac{4}{25}i.$$
11. See Remark after article 8, Theorem 1.
12. See Example 11.
13. See article 8, Theorem 3.
14. In the ring of integers $(\mathbf{I}, +, \bullet)$, the unity element is 1. We have $1.1 = 1$ and $(-1).(-1) = 1$. So, the multiplicative inverse of 1 is 1 and the multiplicative inverse of -1 is -1. Now, if a and b are any two integers, then $ab = 1$ is possible only if $a = 1, b = 1$ or if $a = -1, b = -1$. Thus, the only elements of the ring of integers which possess multiplicative inverse are 1 and -1.
15. See Problem 8 (i) of Comprehensive Problems 1.

16. Since the non-zero elements of a field form an abelian group with respect to multiplication, therefore $(a^{-1})^{-1} = a$.

True or False

1. For example, the ring of integers $(\mathbf{I}, +, \bullet)$ is an integral domain but it is not a field.

2. We know that a field has no zero divisors.
See article 8, Theorem 1.

3. See article 8, Theorem 1.

4. See article 8, Theorem 3.

5. A ring R is said to be a commutative ring if

$$ab = ba\ ,\ \forall\ a, b \in R\ .$$

6. In an arbitrary ring R , we have

$$(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2.$$

In an arbitrary ring R , it is not necessary that $ab = ba$.

7. In a commutative ring R , we have $ab = ba,\ \forall\ a, b \in R$.

So, $(a + b)^2 = a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2 = a^2 + 2\,ab + b^2.$

8. The ring of even integers does not possess multiplicative identity. So, it is a ring without unity.

9. The multiplication of complex numbers is commutative, the complex number $1 + 0i$ *i.e.*, the complex number 1 is the multiplicative identity and every non-zero complex number $x + iy$ possesses the multiplicative inverse

$$\frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}\cdot$$

Hence, the ring of complex numbers is a field.

10. The ring of integers is a commutative ring with unity and without zero divisors. So, it is an integral domain.

11. We have $3 \neq 0, 4 \neq 0$, but $3 \times_6 4 = 0$. So, 3 and 4 are zero divisors.

12. Since 3 is prime, therefore the given ring is a field. We know that a field has no zero divisors.

13. Since 5 is prime, therefore the given ring is a field.

14. We know that if a and b are any two integers, then $ab = 0 \Rightarrow a = 0$ or $b = 0$. Thus, the ring of integers is a ring without zero divisors.

15. See Example 6.

16. See Example 6.

If $A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix}$,

then $AB = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 3 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

= the zero element of the ring while $A \neq 0$ and $B \neq 0$. Thus, the product of two non-zero elements A and B of the ring is equal to the zero element of the ring. So, A and B are zero divisors. Hence, the ring is a ring with zero divisors.

17. In the ring of 2×2 matrices, if $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0$$

while $BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ *i.e.*, $BA \neq 0$.

18. If $a \neq 0$, then $ab = ac \Rightarrow b = c$ is true only if the ring is without zero divisors.

19. See article 5 Theorem.

20. In a field F, the operation of multiplication is commutative. So,

$$ab = 0 \Rightarrow ba = 0 \qquad [\because \; ab = ba, \; \forall \; a, b \in F \;]$$

21. The ring of integers is of characteristic zero. See article 9.

22. The characteristic of a field is either zero or a prime number.

23. See article 11.

24. The characteristic of the field of rational numbers is zero or infinite.

❍❍❍

Chapter-10

Subrings and Ideals

Comprehensive Problems 1

Problem 1: *Show that the set of all 2-rowed matrices of the form* $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ *where a, b, c are integers is a subring of the ring M of all 2-rowed matrices with integral entries.*

Solution: Let M be the set of all 2×2 matrices with elements as integers. Then M is a ring for addition and multiplication of matrices as the two ring operations.

Let S be the subset of M consisting of matrices of the type

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}, \text{ where } a, b, c \text{ are integers.}$$

To prove that S is a subring of the ring M.

Let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & c_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ b_2 & c_2 \end{bmatrix}$ be any two members of the set S.

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & c_1 - c_2 \end{bmatrix}$ which is obviously a member of the set S.

Also $AB = \begin{bmatrix} a_1a_2 & 0 \\ b_1a_2 + c_1b_2 & c_1c_2 \end{bmatrix}$ which is also a member of the set S.

Thus $A, B \in S \Rightarrow A - B \in S$ and $AB \in S$. Hence S is a subring of the ring M.

Problem 2: *Give an example to show that the union of two subrings is not necessarily a subring.*

Solution: Consider the ring of integer $(\mathbf{I}, +, \bullet)$ where

$\mathbf{I} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ is the set of integers.

Let $S_1 = 2\,\mathbf{I} = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$,

$S_2 = 3\,\mathbf{I} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$,

and $S_3 = 4\,\mathbf{I} = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$.

Then S_1, S_2, S_3 are all subrings of the ring of integers.

Now $S_1 \cup S_2$ is not a subring of the ring of integers because $S_1 \cup S_2$ is not closed for addition.

We have $2 \in S_1 \cup S_2$ because $2 \in S_1$ and $3 \in S_1 \cup S_2$ because $3 \in S_2$. But $2 + 3 = 5 \notin S_1 \cup S_2$ because neither $5 \in S_1$ nor $5 \in S_2$. Thus $S_1 \cup S_2$ is not closed for addition. Hence $S_1 \cup S_2$ is not a subring of the ring of integers.

However $S_1 \cup S_3 = S_1$ because $S_3 \subset S_1$. Thus $S_1 \cup S_3$ is a subring of the ring of integers.
From the above example it is obvious that the union of two subrings may or may not be a subring.

Problem 3: *Prove or disprove that any subring of a non-commutative ring is non-commutative.*

Solution: A subring of a non-commutative ring may be commutative as is obvious from the following example.

Let M be the ring of all 2×2 matrices with elements as integers for addition and multiplication of matrices as the two ring operations. Then M is a non-commutative ring because the operation of multiplication of matrices on the set M is not commutative.

Let S be the subset of M consisting of matrices of the type $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ where a is any integer.

Let $A = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}$ be any two members of the set S.

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ 0 & 0 \end{bmatrix} \in S$

and $AB = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \in S.$

$\therefore$ S is a subring of the ring M.

Now the subring S of the ring M is a commutative ring. For let $A = \begin{bmatrix} a_1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 \\ 0 & 0 \end{bmatrix}$ be any two members of S. Then

$$AB = \begin{bmatrix} a_1 a_2 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } BA = \begin{bmatrix} a_2 a_1 & 0 \\ 0 & 0 \end{bmatrix}.$$

Since $a_1 a_2 = a_2 a_1$, therefore $AB = BA$.
Thus multiplication of matrices is a commutative operation on the set S. Hence the subring S of the non-commutative ring M is a commutative ring.

Problem 4: *Show that the set of even integers forms a subring of the ring of integers.*

Solution: Let $(\mathbf{I}, +, \bullet)$ be the ring of integers.

Let $S = 2\,\mathbf{I} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$ be the set of even integers. Then $S \subset \mathbf{I}$.
To prove that S is a subring of the ring of integers.
Let $a = 2r$ and $b = 2s$ be any two elements of S where r and s are some integers.
Then $a - b = 2r - 2s = 2(r - s)$ which is an even integer and so $a - b \in S$.
Also $ab = (2r)(2s) = 2(2rs)$ which is also an even integer and so $ab \in S$.
Thus $a, b \in S \Rightarrow a - b \in S$ and $ab \in S$. Hence the set of even integers S is a subring of the ring of integers.

Problem 5: *If R is a ring , show that $Z(R) = \{x \in R : x\ y = y\ x\ \forall\ y \in R\}$ is subring of R. Further show that $Z(R)$ is a field if R is a division ring.*

Solution: We have $0\ y = 0 = y\ 0\ \forall\ y \in R$. Therefore $0 \in Z(R)$ and so $Z(R) \neq \varnothing$.

Now let $z_1, z_2 \in Z(R)$. Then

$$z_1\ y = y\ z_1 \text{ and } z_2\ y = y\ z_2\ \forall\ y \in R.$$

Now $\forall\ y \in R$, we have

$$(z_1 - z_2)\ y = z_1\ y - z_2\ y$$
$$= y\ z_1 - y\ z_2 = y\ (z_1 - z_2)$$

and
$$(z_1 z_2)\ y = z_1\ (z_2\ y) = z_1\ (y\ z_2)$$
$$= (z_1\ y)\ z_2 = (y\ z_1)\ z_2 = y\ (z_1 z_2).$$

$\therefore$ by definition of $Z(R)$, both $z_1 - z_2$ and $z_1 z_2 \in Z(R)$.

Thus $z_1, z_2 \in Z(R) \Rightarrow z_1 - z_2 \in Z(R)$ and $z_1 z_2 \in Z(R)$.

$\therefore$ $Z(R)$ is a subring of R.

Now suppose R is a division ring *i.e.*, R is a ring with unity and every non-zero element of R possesses multiplicative inverse. Then to prove that $Z(R)$ is a field.

Z (R) is a commutative ring: Let $z_1, z_2 \in Z(R)$.

Now $z_1 \in Z(R) \Rightarrow z_1\ y = y\ z_1\ \forall\ y \in R$. Since $z_2 \in R$, therefore $z_1 z_2 = z_2 z_1$.
Thus $z_1 z_2 = z_2 z_1\ \forall\ z_1, z_2 \in Z(R)$ and so $Z(R)$ is a commutative ring.

The ring Z (R) possesses multiplicative identity: If 1 denotes the unity element of the division ring R, then $1\ y = y = y\ 1\ \forall\ y \in R$. Therefore $1 \in Z(R)$ and is also the unity element of $Z(R)$. Thus $Z(R)$ is also a ring with unity.

Each non-zero element of the ring Z (R) possesses multiplicative inverse: Let $0 \neq z \in Z(R)$ and let z^{-1} denote the multiplicative inverse of z in the division ring R. We shall show that $z^{-1} \in Z(R)$.

We have $z \in Z(R) \Rightarrow z\ y = y\ z\ \forall\ y \in R$

$\Rightarrow$ $z^{-1}\ (z\ y)\ z^{-1} = z^{-1}\ (y\ z)\ z^{-1}\ \forall\ y \in R$

$\Rightarrow$ $(z^{-1} z)\ y\ z^{-1} = (z^{-1}\ y)\ z\ z^{-1}\ \forall\ y \in R$

$\Rightarrow$ $1\ (y\ z^{-1}) = (z^{-1}\ y)\ 1\ \forall\ y \in R$

$\Rightarrow$ $y\ z^{-1} = z^{-1}\ y\ \forall\ y \in R.$

$\therefore$ by the definition of $Z(R)$, $z^{-1} \in Z(R)$.

Since $z\ z^{-1} = 1 = z^{-1}\ z$, where 1 is the unity element of the ring $Z(R)$, therefore z^{-1} is also the multiplicative inverse of z in the ring $Z(R)$.
Thus each non-zero element of the ring $Z(R)$ is inversible.
Since $Z(R)$ is a commutative ring with unity and each non-zero element of $Z(R)$ is inversible, therefore $Z(R)$ is a field.

Comprehensive Problems 2

Problem 1: *Distinguish between Subrings and Ideals in a ring. Show that the 2-rowed matrices of the form* $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$ *where a, b, c are integers form a subring of the ring of all 2-rowed matrices with integral entries. Is this subring an integral domain ?*

Solution: **Distinction between subrings and ideals in a ring:**

Let R be any ring and S be any non-empty subset of R.

So far as the operation of addition is concerned, whether S is a subring or an ideal of R, S must be a subgroup of the additive group of R *i.e.*,

$$a \in S, b \in S \Rightarrow a - b \in S.$$

But so far as the operation of multiplication is concerned, for S to be a subring of R, the product of any two elements of S must remain in S *i.e.*,

$$a \in S, b \in S \Rightarrow ab \in S.$$

While on the other hand for S to be an ideal of R the product of any element of R and any element of S must remain in S *i.e.*,

$$r \in R, s \in S \Rightarrow rs \in S \text{ and } sr \in S.$$

Thus an ideal requires a stronger closure property for multiplication than a subring. **In fact every ideal is a subring while a subring may or may not be an ideal.** For example the set of integers is only a subring but not an ideal of the ring of rational numbers. On the other hand the set of even integers is a subring as well as an ideal of the ring of integers.

Second part of the question: Let M be the ring of all 2×2 matrices with elements as integers for addition and multiplication of matrices as the two ring operations.

Let S be the subset of M consisting of matrices of the form $\begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, where a, b, c are any integers.

To show that S is a subring of M.

Let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & c_1 \end{bmatrix}, B = \begin{bmatrix} a_2 & 0 \\ b_2 & c_2 \end{bmatrix}$ be any two elements of S.

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & c_1 - c_2 \end{bmatrix}$ which is obviously an element of S.

Also $AB = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 + c_1 b_2 & c_1 c_2 \end{bmatrix}$ which is also an element of S.

Hence S is a subring of the ring M.

The subring S of M is not an integral domain because it possesses zero divisors.

The zero element of the subring S is the null matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Now $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are two non-zero elements of S but $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ = the zero element of S. Thus both A and B are zero divisors. Hence S is not an integral domain.

Problem 2: *Show that the set M of all* 2×2 *matrices of the form* $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ *a, b integers is a left ideal but not a right ideal in the ring of all* 2×2 *matrices with elements as integers.*

Solution: Let R be the ring of all 2×2 matrices with elements as integers for addition and multiplication of matrices as the two ring operations. Let M be the subset of R consisting of matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$, where a, b are any integers.

First to show that M is a left ideal of the ring R.

Let $A = \begin{bmatrix} 0 & a_1 \\ 0 & b_1 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & a_2 \\ 0 & b_2 \end{bmatrix}$ be any two elements of M.

Then $A - B = \begin{bmatrix} 0 & a_1 - a_2 \\ 0 & b_1 - b_2 \end{bmatrix} \in M$.

$\therefore$ M is a subgroup of the additive group of the ring R.

Now let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of R and $A = \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ be any element of M.

Then $$UA = \begin{bmatrix} w & x \\ y & z \end{bmatrix}\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$$

$$= \begin{bmatrix} 0 & wa + xb \\ 0 & ya + zb \end{bmatrix} \in M.$$

Therefore M is a left ideal of R.

But M is not a right ideal of R, since

$$\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \in M, \begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix} \in R,$$

and the product $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 3 & 5 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 3 & 5 \end{bmatrix}$ which is not an element of M. Hence M is not a right ideal of R.

Problem 3: *Show that for a field F, the set of all matrices of the form* $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ *for* $a, b \in F$ *is a right ideal but not a left ideal of the ring of all* 2×2 *matrices over the field F.*

Solution: Let R be the ring of all 2×2 matrices with elements in the field F for addition and multiplication of matrices as the two ring operations. Let M be the subset of R consisting of matrices of the form

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a, b \in F.$$

First to show that M is a right ideal of the ring R.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}$ be any two elements of M.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & 0 \end{bmatrix} \in M.$

$\therefore$ M is a subgroup of the additive group of the ring R.

Now let $U = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ be any element of R and $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ be any element of M.

Then $AU = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw + by & ax + bz \\ 0 & 0 \end{bmatrix} \in M.$

Therefore M is a right ideal of the ring R.

But M is not a left ideal of R, since

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in R, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \in M,$$

and the product $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \notin M.$

Hence M is not a left ideal of R.

Problem 4: *Show that S is an ideal of $S + T$ where S is any ideal of ring R and T any subring of R.*

Solution: Since S is an ideal of R therefore S is a subring of R. Also T is a subring of R. First we shall show that $S + T$ is a subring of R. Let $a + \alpha, b + \beta \in S + T$, where $a, b \in S$ and $\alpha, \beta \in T$.

Since S is a subring, therefore $a - b \in S$. Similarly $\alpha - \beta \in T$.

$\therefore$ $(a + \alpha) - (b + \beta) = (a - b) + (\alpha - \beta) \in S + T.$

Also $(a + \alpha)(b + \beta) = ab + a\beta + \alpha b + \alpha\beta = (ab + a\beta + \alpha b) + \alpha\beta.$

Now S is a subring. Therefore $a, b \in S \Rightarrow ab \in S$.

Also S is an ideal, therefore $a, b \in S$ and $\alpha, \beta \in R \Rightarrow a\beta, \alpha b \in S$. Therefore $ab + a\beta + \alpha b \in S$.

Further T is a subring implies $\alpha\beta \in T$ if $\alpha, \beta \in T$.

$\therefore$ $(a + \alpha)(b + \beta) = (ab + a\beta + \alpha b) + \alpha\beta \in S + T.$

$\therefore$ $S + T$ is a subring of R.

Since $0 \in T$, therefore $a \in S$ can be written as

$$a = a + 0 \in S + T.$$

$$\therefore \quad S \subseteq S + T.$$

Thus $S \subseteq S + T$ and $S + T$ is a subring of R. Since S is an ideal of R, therefore S is also an ideal of $S + T$.

Problem 5: *If U is a left ideal of a ring R, let*

$$\lambda(U) = \{x \in R : xu = 0 \ \forall \ u \in U\}.$$

Prove that $\lambda(U)$ is a two sided ideal of R.

Solution: First we see that $\lambda(U) \neq \varnothing$ because $0 \in R$ is such that

$$0u = 0 \ \forall \ u \in U.$$

Now let x_1, x_2 be any two elements of $\lambda(U)$. Then

$$x_1 u = 0 \ \forall \ u \in U \text{ and } x_2 u = 0 \ \forall \ u \in U.$$

We have $(x_1 - x_2)u = x_1 u - x_2 u = 0 - 0 = 0$ for all $u \in U$.

$$\therefore \quad x_1 - x_2 \in \lambda(U).$$

Now let x be any element of $\lambda(U)$ and r be any element of R.

Then $\quad xu = 0 \ \forall \ u \in U$ [By def. of $\lambda(U)$]

$$\Rightarrow \quad r(xu) = r\,0 \ \forall \ u \in U$$

$$\Rightarrow \quad (rx)u = 0 \text{ for all } u \in U \Rightarrow rx \in \lambda(U).$$

Further U is a left ideal of R. Therefore $ru \in U \ \forall \ u \in U$.

Since $x \in \lambda(U)$, therefore by def. of $\lambda(U)$, we have

$$x \in \lambda(U), ru \in U \Rightarrow x(ru) = 0 \text{ for all } u \in U$$

$$\Rightarrow \quad (xr)u = 0 \text{ for all } u \in U$$

$$\Rightarrow \quad xr \in \lambda(U).$$

Thus $\quad x \in \lambda(U), r \in R \Rightarrow xr, rx \in \lambda(U).$

Hence $\lambda(U)$ is a two sided ideal of R.

Problem 6: *If U, V are ideals of a ring R let UV be the set of all those elements of R which can be written as finite sums of elements of the form uv where $u \in U$ and $v \in V$. Prove that UV is an ideal of R. Also show that $UV \subseteq U \cap V$.*

Solution: U and V are ideals of a ring R. Let

$$UV = \{u_1 v_1 + u_2 v_2 + \ldots + u_n v_n : u_1, u_2, \ldots, u_n \in U, v_1, v_2, \ldots, v_n \in V$$

and n is any positive integer}.

To prove that UV is also an ideal of R.

Let $\quad \alpha = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n,$

$$\beta = u_1' v_1' + u_2' v_2' + \ldots + u_m' v_m'$$

be any two elements of UV, where $u_1, u_2, \ldots, u_n, u_1', u_2', \ldots, u_m' \in U$

and $\quad v_1, v_2, \ldots, v_n, v_1', v_2', \ldots, v_m' \in V.$

Also m and n are any positive integers.

We have $\alpha - \beta = u_1 v_1 + u_2 v_2 + \ldots + u_n v_n - u_1' v_1' - u_2' v_2' - \ldots - u_m' v_m'$

$= u_1 v_1 + u_2 v_2 + \ldots + u_n v_n + (-u_1') v_1' + (-u_2') v_2' + \ldots + (-u_m') v_m'.$

This is obviously an element of UV because U is an ideal and therefore

$u_1' \in U \Rightarrow (-u_1') \in U$, etc.

Again let $r \in R$ and $\alpha \in UV$. Then

$r\alpha = r(u_1v_1 + u_2v_2 + \ldots + u_nv_n) = (r u_1) v_1 + (r u_2) v_2 + \ldots + (r u_n) v_n$

This is an element of UV because U is an ideal and therefore $r \in R, u_1 \in U \Rightarrow r u_1 \in U$, etc.

Also $\alpha r = (u_1 v_1 + u_2 v_2 + \ldots + u_n v_n) r$

$= u_1 (v_1 r) + u_2 (v_2 r) + \ldots + u_n (v_n r).$

This is an element of UV because V is an ideal and therefore

$r \in R, v_1 \in V \Rightarrow v_1 r \in V$, etc.

Hence UV is an ideal of R.

Now to show that $UV \subseteq U \cap V$.

Let $\alpha = u_1 v_1 + \ldots + u_n v_n$ be any element of UV where

$u_1, \ldots, u_n \in U$ and $v_1, \ldots, v_n \in V$.

Now $v_1 \in V \Rightarrow v_1 \in R$. Also U is an ideal. Therefore

$v_1 \in R, u_1 \in U \Rightarrow u_1 v_1 \in U$.

Similarly $u_1 \in U \Rightarrow u_1 \in R$. But V is an ideal. Therefore

$u_1 \in R, v_1 \in V \Rightarrow u_1 v_1 \in V$.

Thus $u_1 v_1 \in U, u_1 v_1 \in V \Rightarrow u_1 v_1 \in U \cap V$.

Similarly $u_2 v_2, \ldots, u_n v_n \in U \cap V$.

Since $U \cap V$ is also an ideal of R, therefore

$u_1 v_1, \ldots, u_n v_n \in U \cap V \Rightarrow \alpha = u_1 v_1 + \ldots + u_n v_n \in U \cap V$.

Thus $\alpha \in UV \Rightarrow \alpha \in U \cap V$. Therefore $UV \subseteq U \cap V$.

Problem 7: *If U, V are ideals of a ring R, let $U + V = \{u + v : u \in U, v \in V\}$.*

Prove that $U + V$ is also an ideal of R.

Solution: Let $u_1 + v_1 \in U + V$ and $u_2 + v_2 \in U + V$. Then

$u_1, u_2 \in U$ and $v_1, v_2 \in V$.

We have $(u_1 + v_1) - (u_2 + v_2) = (u_1 - u_2) + (v_1 - v_2)$.

Since U is an ideal of R, therefore

$u_1, u_2 \in U \Rightarrow u_1 - u_2 \in U$.

Similarly V is also an ideal of R, therefore

$v_1, v_2 \in V \Rightarrow v_1 - v_2 \in V$.

$\therefore \quad (u_1 - u_2) + (v_1 - v_2) \in U + V$.

$\therefore \quad (u_1 + v_1) - (u_2 + v_2) \in U + V$.

$\therefore$ $U + V$ is a subgroup of the additive group of R.

Now let r be any element of R and $u + v$ be any element of $U + V$ where $u \in U, v \in V$.

Then $r(u + v) = ru + rv \in U + V$ since $r \in R, u \in U$ and U is an ideal

$\Rightarrow$ $ru \in U$ and similarly $rv \in V$.

Similarly $(u + v)r = ur + vr \in U + V$ since $ur \in U, vr \in V$.

Hence $U + V$ is an ideal of R.

Problem 8: *Show that an arbitrary intersection of ideals of a ring is an ideal of the ring.*

Solution: Let R be a ring and let $\{S_t : t \in T\}$ be any family of ideals of R. Here T is an index set and is such that $\forall\ t \in T$, S_t is an ideal of R.

Let $S = \underset{t \in T}{\cap} S_t = \{x \in R : x \in S_t\ \forall\ t \in T\}$

be the intersection of this family of ideals of R. Then to prove that S is also an ideal of R.

Obviously $S \neq \varnothing$, since at least 0 is in $S_t\ \forall\ t \in T$.

Now let a, b be any two elements of S. Then

$a, b \in S \Rightarrow a, b \in S_t\ \forall\ t \in T$

$\Rightarrow$ $a - b \in S_t\ \forall\ t \in T$ $[\because \forall\ t \in T, S_t$ is an ideal of $R]$

$\Rightarrow$ $a - b \in \underset{t \in T}{\cap} S_t \Rightarrow a - b \in S$.

$\therefore$ S is a subgroup of the additive group of R.

Now let s be any element of S and r be any element of R.

We have $s \in S \Rightarrow s \in \underset{t \in T}{\cap} S_t \Rightarrow s\ S_t\ \forall\ t \in T$

$\Rightarrow$ $rs \in S_t$ and $sr \in S_t\ \forall\ t \in T$ $[\because \forall\ t \in T, S_t$ is an ideal of $R]$

$\Rightarrow$ $rs \in \underset{t \in T}{\cap} S_t$ and $sr \in \underset{t \in T}{\cap} S_t$

$\Rightarrow$ $rs \in S$ and $sr \in S$.

Thus $a, b \in S \Rightarrow a - b \in S$ and $r \in R$, $s \in S \Rightarrow rs \in S, sr \in S$.

Hence S is an ideal of the ring R.

Problem 9: *If U is an ideal of a ring R, let $r(U) = \{x \in R : xu = 0\ \forall\ u \in U\}$.*

Prove that $r(U)$ is an ideal of R.

Solution: Proceed exactly as in problem 5. While giving the proof simply replace the words 'left ideal' by 'ideal'.

Problem 10: *Consider the ring R of all 3×3 matrices of the type* $\begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$,

a, b, c, d, e, f are real numbers. Show that the set I of all matrices of the form $\begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$,

is a left ideal of R, which is not a right ideal.

Solution: First to show that **I** is a left ideal of R.

Let $A = \begin{bmatrix} a_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ be any two elements of **I.**

Then $A - B = \begin{bmatrix} a_1 - a_2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in \mathbf{I}.$

$\therefore$ **I** is a subgroup of the additive group of the ring R.

Now let $U = \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}$ be any element of R

and $A = \begin{bmatrix} p & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ be any element of **I.**

Then $UA = \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix}\begin{bmatrix} p & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} ap & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in \mathbf{I}.$

Therefore **I** is a left ideal of the ring R.

But **I** is not a right ideal of R, since

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \in R, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \in \mathbf{I},$$

and the product

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \notin \mathbf{I}.$$

Hence **I** is not a right ideal of R.

Problem 11: *Verify the following for being true or false :*

(i) The set of all positive rationals is a subring of the ring of all rational numbers.

(ii) A subring of any field is a field.

(iii) Any subring of the ring of integers, Z, is an ideal of Z.

Solution: (i) Let $(\mathbf{Q}, +, \bullet)$ be the ring of all rational numbers and $\mathbf{Q}_+$ be the set of all positive rational numbers.

Then $\mathbf{Q}_+$ is not a subring of the ring $(\mathbf{Q}, +, \bullet)$. Obviously the rational number 0 which is the zero element of the ring of all rational numbers does not belong to $\mathbf{Q}_+$. Therefore $\mathbf{Q}_+$ is not a subring of the ring $(\mathbf{Q}, +, \bullet)$. Hence the given statement is false.

(ii) The statement that a subring of any field is a field is false. For example consider the field of rational numbers $(\mathbf{Q}, +, \bullet)$. The set of integers $\mathbf{I}$ is a subring of the field of rational numbers because $a \in \mathbf{I}, b \in \mathbf{I} \Rightarrow a - b \in \mathbf{I}$ and $ab \in \mathbf{I}$.

But the subring $(\mathbf{I}, +, \bullet)$ of the field $(\mathbf{Q}, +, \bullet)$ is not a field. The only elements in $\mathbf{I}$ which possess multiplicative inverse are 1 and – 1 while in a field every non-zero element must possess multiplicative inverse. Hence $(\mathbf{I}, +, \bullet)$ is not a field and so the given statement is false.

(iii) The statement that any subring of the ring of integers, Z, is an ideal of Z is true.

If S is the zero subring of Z, then obviously S is an ideal of Z.

If S is any subring other than the zero subring of the ring of integers Z and m is the smallest positive integer belonging to S, then we have

$$S = \{xm : x \text{ is an integer}\}.$$

Now show that S is an ideal of the ring Z as we have done in solved Example 6.

Hence any subring of the ring of integers, Z, is also an ideal of Z.

Comprehensive Problems 3

Problem 1: *Show that every homomorphic image of a commutative ring is commutative.*

Solution: Let R be a commutative ring. Let f be a homomorphic mapping of R onto a ring R'. Then R' is a homomorphic image of R.

Let a', b' be any two elements of R'. Then $f(a) = a'$, $f(b) = b'$ for some $a, b \in R$ because f is onto R'. We have

$$a'b' = f(a)\, f(b) = f(ab) = f(ba) \qquad [\because R \text{ is commutative}]$$
$$= f(b)\, f(a) = b'a'.$$

$\therefore$ R' is a commutative ring.

Problem 2: *If R is a ring with unit element 1 and ϕ is a homomorphism of R onto R' prove that $\phi(1)$ is the unity element of R'.*

Solution: Since ϕ is a homomorphism of R onto R', therefore R' is a homomorphic image of R. If 1 is the unity element of R, then $\phi(1) \in R'$. Let a' be any element of R'. Then $a' = \phi(a)$ for some $a \in R$ since ϕ is onto R'. We have

$$\phi(1)\, a' = \phi(1)\, \phi(a) = \phi(1a) = \phi(a) = a'$$

and
$$a'\phi(1) = \phi(a)\, \phi(1) = \phi(a1) = \phi(a) = a'.$$

$\therefore$ $\phi(1)$ is the unity element of R'.

Problem 3: *If R is a ring with unit element 1 and ϕ is a homomorphism of R into an integral domain R' such that kernel of ϕ i.e., $I(\phi) \neq R$, then prove that $\phi(1)$ is the unity element of R'.*

Solution: ϕ is a homomorphism of a ring R into an integral domain R'. Then kernel of ϕ

$$= I(\phi) = \{x : x \in R \text{ and } \phi(x) = 0 \in R'\}.$$

Since $I(\phi) \neq R$, therefore there exists an element $a \in R$ such that

$$\phi(a) \neq 0 \in R'.$$

We have $\phi(1)\,\phi(a) = \phi(1a) = \phi(a)$.

Now let b' be any element of R'. We have

$$\phi(a)\,b' = \phi(a)\,b'$$

$\Rightarrow$ $\phi(1)\,\phi(a)\,b' = \phi(a)\,b'$ $[\because\ \phi(1)\,\phi(a) = \phi(a)]$

$\Rightarrow$ $\phi(a)[\phi(1)\,b'] = \phi(a)\,b'$ $[\because\ \phi(1), \phi(a) \in R'$ which, being an integral domain, is a commutative ring]

$\Rightarrow$ $\phi(a)\,[\phi(1)\,b'] - \phi(a)\,b' = 0$

$\Rightarrow$ $\phi(a)\,[\phi(1)\,b' - b'] = 0$

$\Rightarrow$ $\phi(1)\,b' - b' = 0$ $[\because\ \phi(a) \neq 0$ and R' is without zero divisors]

$\Rightarrow$ $\phi(1)\,b' = b' = b'\,\phi(1)$. $[\because R'$ is a commutative ring]

Thus $\phi(1)\,b' = b' = b'\,\phi(1)\ \forall\ b' \in R'$.

$\therefore$ $\phi(1)$ is the unity element of R'.

Problem 4: *Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.*

Or

Show that a field has no proper homomorphic image.

Solution: Let ϕ be a homomorphism of a field F into a ring R. Let S be the kernel of ϕ. Then S is an ideal of the field F. We know that a field has no proper ideals. Therefore either $S = F$ or $S = (0)$.

If $S = F$, then by definition of kernel of ϕ, we have $\phi(x) = 0\ \forall\ x \in F$. Thus in this case ϕ takes each element of F into the zero element of R. In other words in this case $\phi(F)$ is the zero subring of the ring R.

If $S = (0)$, then the kernel consists of zero element alone. So in this case ϕ is an isomorphism of F into R. [See theorem 2 of article 9]. Since the isomorphic image of a field is a field, therefore in this case $\phi(F)$ is a field isomorphic to the field F.

Hints to Objective Type Questions

Multiple Choice Questions

1. See Example 9.
2. See article 1.
3. See article 2.
4. See article 3.
5. See article 3, Note 2.
6. See Example 8.
7. See Example 7.

8. See Theorem 2 of article 1 and Example 1.
9. See article 6, Theorem 2.
10. See article 22.
11. The set of odd integers is not a ring of **I**.
12. See Example 17.
13. We know that the union of two subrings S_1 and S_2 is a subring if and only if one is contained in the other *i.e.*, if and only if $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.
14. See article 23.
15. See article 3.

Fill in the Blank(s)

1. See article 1, Theorem 1.
2. See article 2, conditions for a subfield.
3. We know that the union of two subrings S_1 and S_2 is a subring if and only if one is contained in the other *i.e.*, if and only if $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.
4. See article 1, conditions for a subring.
5. See article 3, Note 2.
6. See article 1.
7. See article 8, Definition of Principal Ideal.

True or False

1. The set of positive rational numbers $\mathbf{Q}^+$ is not a subring of the ring of rational numbers **Q**. Obviously, the zero element $0 \approx \mathbf{Q}^+$.
2. The ring of integers is a subring of the field of rational numbers but it is not a subfield of the field of rational numbers. Its only inversible elements are 1 and -1 while in a field every non-zero element must be inversible.
3. Since $\mathbf{Q} \subset \mathbf{R}$ and the rational numbers form a field for addition and multiplication of real numbers, therefore the field of rational numbers is a subfield of the field of real numbers.
4. See the reasons given in Question 2 of True or False.
5. See Problem 2 of Comprehensive Problems 1.
6. See Example 4.
7. Except 0, no other element of S possesses additive inverse. So, S is not a subring of the ring of integers.

○○○

Chapter-11

Polynomial Rings and Unique Factorization Domain

Comprehensive Problems 1

Problem 1: *Resolve* $x^4 + 4$ *into factors over the field* $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

Solution: Let F be the field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

Let $f(x) = x^4 + 4 \in F\,[\,x\,]$.

We have $f(0) = 0^4 +_5 4 = 4 \neq 0, \quad f(1) = 1^4 +_5 4 = 1 +_5 4 = 0,$

$f(2) = 2^4 +_5 4 = (2 \times_5 2 \times_5 2 \times_5 2) +_5 4 = 1 +_5 4 = 0,$

$f(3) = 3^4 +_5 4 = 1 +_5 4 = 0$ and $f(4) = 4^4 +_5 4 = 1 +_5 4 = 0.$

By factor theorem, we know that if $f(x)$ is a polynomial over the field F and $a \in F$, then $x - a$ is a factor of $f(x)$ iff $f(a) = 0$.

So the only factors of $f(x)$ over the given field F are $x - 1$, $x - 2$, $x - 3$ and $x - 4$.

Now in the given field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$, we have $1 +_5 4 = 0$ and $2 +_5 3 = 0$.

$\therefore \quad -1 = 4$ and $-4 = 1$.

Also $-2 = 3$ and $-3 = 2$.

Thus over the given field F, we have

$$x - 1 = x + 4,\ x - 2 = x + 3, x - 3 = x + 2 \text{ and } x - 4 = x + 1.$$

Hence over the given field $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$, we have

$$x^4 + 4 = (x + 1)(x + 2)(x + 3)(x + 4).$$

Problem 2: *Resolve* $x^2 + 1$ *into factors over the field* Z_5.

Solution: The field Z_5 is $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

Let $f(x) = x^2 + 1.$

We have $f(0) = 0^2 +_5 1 = 1 \neq 0, \ f(1) = 1^2 +_5 1 = 2 \neq 0,$

$f(2) = 2^2 +_5 1 = 4 +_5 1 = 0,$

$f(3) = 3^2 +_5 1 = (3 \times_5 3) +_5 1 = 4 +_5 1 = 0,$

$f(4) = 4^2 +_5 1 = (4 \times_5 4) +_5 1 = 1 +_5 1 = 2 \neq 0.$

By factor theorem, we know that if $f(x)$ is a polynomial over the field F and $a \in F$, then $x - a$ divides $f(x)$ if and only if $f(a) = 0$.

So the only factors of $f(x) = x^2 + 1$ over the field Z_5 are $x - 2$ and $x - 3$.

Here -2 and -3 are the additive inverses of 2 and 3 respectively in the field Z_5. In the

field Z_5, we have $2 +_5 3 = 0$.

$\therefore \quad -2 = 3 \quad$ and $\quad -3 = 2$.

So over the field Z_5, we have

$$x - 2 = x + 3 \text{ and } x - 3 = x + 2.$$

Thus over the field Z_5, we have

$$x^2 + 1 = (x - 2)(x - 3) = (x + 3)(x + 2).$$

Problem 3: *Find the solution of the equation* $3x = 2$ *in the field* $(Z_7, +_7, \times_7)$.

Solution: The field $(Z_7, +_7, \times_7)$ is the field $(\{0, 1, 2, 3, 4, 5, 6\}, +_7, \times_7)$.

If $x \in Z_7$ and $x = 3$, we have

$$3x = x +_7 x +_7 x = 3 +_7 3 +_7 3 = 2.$$

Thus $x = 3$ is a solution of the equation $3x = 2$ in the field $(Z_7, +_7, \times_7)$.

Also no other element of the field Z_7 satisfies the equation $3x = 2$.

If $x = 0$, we have $3x = 0$,
if $x = 1$, we have $3x = 3$,
if $x = 2$, we have $3x = 6$,
if $x = 4$, we have $3x = 5$,
if $x = 5$, we have $3x = 1$,
and if $x = 6$, we have $3x = 4$.

Hence $x = 3$ is the only solution of the equation $3x = 2$ in the given field $(Z_7, +_7, \times_7)$.

Problem 4: *Show that* $f(x) = x^2 + 8x - 2$ *is irreducible over the field of rational numbers* **Q.** *Is it irreducible over reals ? Give reasons for your answer.*

Solution: First we solve the equation $f(x) = 0$ over the field **C** of complex numbers.

We have $\quad x^2 + 8x - 2 = 0$

$$\Leftrightarrow \qquad x = \frac{-8 \pm \sqrt{(64 + 8)}}{2} = -4 \pm 3\sqrt{2}.$$

Thus the only proper factors of $f(x) = x^2 + 8x - 2$ over the field of complex numbers are $x - (-4 + 3\sqrt{2})$ and $x - (-4 - 3\sqrt{2})$.

Since neither $-4 + 3\sqrt{2}$ nor $-4 - 3\sqrt{2}$ is a rational number, therefore neither $x - (-4 + 3\sqrt{2})$ nor $x - (-4 - 3\sqrt{2})$ is a polynomial over the field **Q**. Hence $f(x)$ has no proper factor over the field of rational numbers **Q** and so $f(x)$ is irreducible over the field **Q**.

But both $-4 + 3\sqrt{2}$ and $-4 - 3\sqrt{2}$ are real numbers and so both $x - (-4 + 3\sqrt{2})$ and $x - (-4 - 3\sqrt{2})$ are polynomials over the field of real numbers **R.** Thus $x - (-4 + 3\sqrt{2})$ and $x - (-4 - 3\sqrt{2})$ are proper factors of $f(x) = x^2 + 8x - 2$ over the field of real numbers **R**. Hence $f(x) = x^2 + 8x - 2$ is reducible over the field **R**.

So $f(x) = x^2 + 8x - 2$ is not irreducible over the field of real numbers **R**.

Problem 5: *Let* $f(x) = 2x^4 + 3x^3 + 2$ *and* $g(x) = 3x^5 + 4x^3 + 2x^2 + 3$ *be two polynomials over the field* $Z_5 = (\{0, 1, 2, 3, 4\}, +_5, \times_5)$.

Determine (i) $\frac{d}{dx} f(x)$, *(ii)* $f(x) \cdot g(x)$.

Solution: (*i*) We have

$$\frac{d}{dx} f(x) = 4(2)x^3 + 3(3)x^2$$

$$= (2 +_5 2 +_5 2 +_5 2)x^3 + (3 +_5 3 +_5 3)x^2 = 3x^3 + 4x^2.$$

(*ii*) We have $f(x)\, g(x) = (2 + 3x^3 + 2x^4)(3 + 2x^2 + 4x^3 + 3x^5)$

$$= (2 \times_5 3) + (2 \times_5 2)x^2 + [(2 \times_5 4) +_5 (3 \times_5 3)]x^3$$
$$+ (2 \times_5 3)x^4 + [(2 \times_5 3) +_5 (3 \times_5 2)]x^5$$
$$+ [(3 \times_5 4) +_5 (2 \times_5 2)]x^6 + (2 \times_5 4)x^7$$
$$+ (3 \times_5 3)x^8 + (2 \times_5 3)x^9$$
$$= 1 + 4x^2 + 2x^3 + x^4 + 2x^5 + x^6 + 3x^7 + 4x^8 + x^9.$$

Problem 6: *If* $f(x) = 3x^7 + 2x + 3$, $g(x) = 5x^3 + 2x + 6$ *be two polynomials over the field* $Z_7 = (\{0, 1, 2, 3, 4, 5, 6\}, +_7, \times_7)$, *determine*

(i) $\frac{d}{dx} f(x)$, *(ii)* $f(x) \cdot g(x)$, *and (iii)* $f(x) + g(x)$.

Solution: (i) We have

$$\frac{d}{dx} f(x) = (7 +_7 7 +_7 7)x^6 + (1 +_7 1) = 0\ x^6 + 2 = 2.$$

(ii) We have $f(x)\, g(x) = (3 + 2x + 3x^7)(6 + 2x + 5x^3)$

$$= (3 \times_7 6) + [(3 \times_7 2) +_7 (2 \times_7 6)]x + (2 \times_7 2)x^2$$
$$+ (3 \times_7 5)x^3 + (2 \times_7 5)x^4 + (3 \times_7 6)x^7$$
$$+ (3 \times_7 2)x^8 + (3 \times_7 5)x^{10}$$
$$= 4 + 4x + 4x^2 + x^3 + 3x^4 + 4x^7 + 6x^8 + x^{10}.$$

(iii) We have $f(x) + g(x) = (3 + 2x + 3x^7) + (6 + 2x + 5x^3)$

$$= (3 +_7 6) + (2 +_7 2)x + (0 +_7 5)x^3 + (3 +_7 0)x^7$$
$$= 2 + 4x + 5x^3 + 3x^7 = 3x^7 + 5x^3 + 4x + 2.$$

Problem 7: *Let* $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ *and* $g(x) = x^2 + 2x - 3$ *be in* $Z_7[x]$. *Find*

(i) Sum and product of $f(x)$ *and* $g(x)$ *in* $Z_7[x]$.

(ii) Two polynomials $q(x)$ *and* $r(x)$ *in* $Z_7[x]$ *such that*

$f(x) = q(x)\, g(x) + r(x)$ *with degree* $r(x) < 2$.

Solution: The field Z_7 is $(\{0,1,2,3,4,5,6\}, +_7, \times_7)$.

In Z_7, $3 +_7 4 = 0$ so that $4 = -3$.

$\therefore$ we can write $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$

$= x^6 + 3x^5 + 4x^2 + 4x + 2$

and $g(x) = x^2 + 2x - 3 = x^2 + 2x + 4$.

(i) We have $f(x) + g(x) = (2 + 4x + 4x^2 + 3x^5 + x^6) + (4 + 2x + x^2)$

$= (2 +_7 4) + (4 +_7 2)\, x + (4 +_7 1)\, x^2 + 3x^5 + x^6$

$= 6 + 6x + 5x^2 + 3x^5 + x^6 = x^6 + 3x^5 + 5x^2 + 6x + 6.$

Also $f(x)\, g(x) = (2 + 4x + 4x^2 + 3x^5 + x^6)(4 + 2x + x^2)$

$= (2 \times_7 4) + [(2 \times_7 2) +_7 (4 \times_7 4)]\, x + [(2 \times_7 1) +_7 (4 \times_7 2)$
$+_7 (4 \times_7 4)]\, x^2 + [(4 \times_7 1) +_7 (4 \times_7 2)]\, x^3 + (4 \times_7 1)\, x^4$
$+ (3 \times_7 4)\, x^5 + [(3 \times_7 2) +_7 (1 \times_7 4)]\, x^6$
$+ [(3 \times_7 1) +_7 (1 \times_7 2)]\, x^7 + (1 \times_7 1)\, x^8$

$= 1 + 6x + 5x^2 + 5x^3 + 4x^4 + 5x^5 + 3x^6 + 5x^7 + x^8$

$= x^8 + 5x^7 + 3x^6 + 5x^5 + 4x^4 + 5x^3 + 5x^2 + 6x + 1.$

In $Z_7[x]$, let us divide $f(x)$ by $g(x)$ by long division method.

$$
\begin{array}{r}
x^4 + x^3 + x^2 + x + 5 \\
x^2 + 2x + 4 \overline{)\; x^6 + 3x^5 + 4x^2 + 4x + 2} \\
\underline{x^6 + 2x^5 + 4x^4} \\
x^5 + 3x^4 + 4x^2 + 4x + 2 \\
\underline{x^5 + 2x^4 + 4x^3} \\
x^4 + 3x^3 + 4x^2 + 4x + 2 \\
\underline{x^4 + 2x^3 + 4x^2} \\
x^3 + 4x + 2 \\
\underline{x^3 + 2x^2 + 4x} \\
5x^2 + 2 \\
\underline{5x^2 + 3x + 6} \\
4x + 3
\end{array}
$$

$[\because$ in Z_7, $3 - 2 = 3 +_7 (-2)$
$= 3 +_7 5 = 1$, $-4 = 3]$

$[\because$ in Z_7, $-4 = 3]$

$[\because$ in Z_7, $-2 = 5]$

$[\because$ in Z_7, $5(2) = 3$
and $5(4) = 6]$

$[\because$ in Z_7, $-3 = 4$ and
$2 - 6 = 2 +_7 (-6) = 2 +_7 1 = 3]$

(ii) The degree of the remainder $4x + 3$ is 1 which is less than 2 *i.e.*, the degree of the divisor $g(x) = x^2 + 2x + 4$.

Thus we have $x^6 + 3x^5 + 4x^2 + 4x + 2 = (x^4 + x^3 + x^2 + x + 5)(x^2 + 2x + 4) + 4x + 3$

i.e., $f(x) = q(x)\, g(x) + r(x)$,

where the quotient $q(x) = x^4 + x^3 + x^2 + x + 5$

and the remainder $r(x) = 4x + 3$.

Comprehensive Problems 2

Problem 1: *If p is a prime number, prove that the polynomial $x^n - p$ is irreducible over the field of rational numbers.* **(Gorakhpur 2013)**

Solution: Let $f(x) = x^n - p = -p + 0x + 0x^2 + ... + 0x^{n-1} + 1x^n$.

Then $f(x)$ is a polynomial with integer coefficients.

Now p is a prime number.

We see that p divides each of the coefficients of $f(x)$ except the coefficient 1 of the last term x^n. Also p^2 is not a divisor of the constant term $-p$. Hence by Eisenstein's criterion of irreducibility $f(x)$ is irreducible over the field of rational numbers.

Problem 2: *Show that the polynomial $x^2 - 3$ is irreducible over the field of rational numbers.*

Solution: Let $f(x) = x^2 - 3 = -3 + 0x + 1x^2$.

Now $f(x)$ is a polynomial with integer coefficients. Also 3 is a prime number such that 3 divides each of the coefficients of $f(x)$ except the coefficient 1 of the last term x^2. Also 3^2 is not a divisor of the constant term -3. Hence by Eisenstein's criterion of irreducibility $f(x)$ is irreducible over the field of rational numbers.

Problem 3: *Prove that the polynomial $1 + x + \ldots + x^{p-1}$, where p is a prime number, is irreducible over the field of rational numbers.*

Solution: Let $f(x) = 1 + x + \ldots + x^{p-1}$.

Multiplying both sides by $x - 1$, we get

$$(x-1)\, f(x) = (x-1)(x^{p-1} + x^{p-2} + ... + x + 1)$$

$$\Rightarrow \quad (x-1)\, f(x) = x^p - 1.$$

Putting $x - 1 = y$ or $x = y + 1$ on both sides, we get

$$y\, f(y+1) = (y+1)^p - 1$$

$$= y^p + {}^pC_1\, y^{p-1} + {}^pC_2\, y^{p-2} + \ldots + {}^pC_{p-1}\, y + 1 - 1,$$

expanding by binomial theorem

$$= y^p + {}^pC_1\, y^{p-1} + {}^pC_2\, y^{p-2} + \ldots + {}^pC_{p-1}\, y$$

$$= y\,[\, y^{p-1} + {}^pC_1\, y^{p-2} + {}^pC_2\, y^{p-3} + \ldots + {}^pC_{p-2}\, y + {}^pC_{p-1}].$$

$$\therefore \quad f(y+1) = y^{p-1} + {}^pC_1\, y^{p-2} + {}^pC_2\, y^{p-3} + \ldots + {}^pC_{p-2}\, y + {}^pC_{p-1}.$$

Now $${}^{p}C_{r} = \frac{p\ (p-1)(p-2)\ldots(p-r+1)}{r!}, 1 \le r \le p-1.$$

Obviously ${}^{p}C_{r}$ is divisible by p for each $1 \le r \le p-1$. Note that p is given to be a prime integer.

Now $f(y+1)$ is a polynomial with integer coefficients. Also p is a prime number such that p divides each of the coefficients of $f(y+1)$ except the coefficient of y^{p-1} which is 1. Also p^2 is not a divisor of the constant term which is equal to ${}^{p}C_{p-1} = p$. Therefore by Eienstein's criterion of irreducibility $f(y+1)$ is irreducible over the field of rational numbers. Therefore $f(x)$ is irreducible over the field of rational numbers. Note that $y = x - 1$.

Problem 4: *Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible over the field of rational numbers.*

Solution: The number 5 is a prime number. So proceed as in Problem 3 by taking $p = 5$.

Problem 5: *Let R be a unique factorization domain. Then show that every prime element in R generates a prime ideal.*

Solution: Let p be a prime element of a unique factorization domain R. Let $S = (p)$ be the ideal of R generated by p. Then to show that S is a prime ideal.

Suppose ab is an element of S where $a, b \in R$. We have

$ab \in S \Rightarrow ab = kp$ for some $k \in R \quad \Rightarrow \quad p \mid ab$

$\Rightarrow \quad p \mid a$ or $p \mid b \quad [\because p$ is a prime element of $R]$

$\Rightarrow \quad a = sp$ or $b = tp$ for some $s, t \in R$

$\Rightarrow \quad a \in (p)$ or $b \in (p) \quad \Rightarrow \quad (p)$ is a prime ideal of R.

Hints to Objective Type Questions

Multiple Choice Questions

1. See article 6, Corollary 2 of Theorem.
2. See article 13.
3. See article 20, Corollary of Factor Theorem.
4. See Example 5 part (i).
5. See article 25, Theorem 6 part (i).
6. See article 25, Theorem 7.
7. See article 21.
8. See Example 6.
9. See article 10.
10. See article 25, Theorem 2.
11. See Example 2.

12. See Example 5.
13. See Example 2.
14. See Example 12, Example 14, Theorem 2 of article 25.
15. See article 25, Theorem 7.
16. See Example 9.
17. See article 25, Theorem 6.

Fill in the Blank(s)

1. See article 8.
2. See article 15.
3. See article 20, Remainder Theorem.
4. See article 21, Theorem.
5. See article 25, Theorem 1.
6. See article 25, Theorem 2.

True or False

1. See article 10, Theorem 2.
2. See Example 6.
3. The field of real numbers is not a prime field. It has a subfield other than itself namely the field of rational numbers.
4. See article 25, Note of Theorem 9.
5. The ring of Gaussian integers is a Euclidean ring. See Example 15.
6. See Example 14.

○○○